ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Centro de Educación Continua

Diplomado en Auditoría Informática

I Promoción

"DISEÑO DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION EN EL CENTRO DE SERVICIOS INFORMATICOS DE LA ESCUELA SUPERIOR POLITECNICA DEL LITORAL (CSI - ESPOL)."

PARTICIPANTES:

Chang Aguilar Miguel Ángel

Noboa Macías Dalton Geovanny

Murrieta Franco Ernesto Napoleón

2006

ESCUELA SUPERIOR POLITECNICA DEL LITORAL

CENTRO DE EDUCACION CONTINUA

DIPLOMADO EN AUDITORIA INFORMATICA

I PROMOCION

"DISEÑO DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION EN EL CENTRO DE SERVICIOS INFORMATICOS DE LA ESCUELA SUPERIOR POLITECNICA DEL LITORAL (CSI – ESPOL)."

PARTICIPANTES:
Chang Aguilar Miguel Ángel
Noboa Macias Dalton Geovanny
Murrieta Franco Ernesto Napoleón

2006

AGRADECIMIENTO

A todas las personas que de
uno u otro modo colaboraron
en la realización de este trabajo
a Jorge y las autoridades
de ESPOL por brindarnos
toda su colaboración

DEDICATORIA

A Dios.

A nuestros padres.

A Grace Aguilar.
Miguel Chang A.

Para Lisette una persona
muy especial para mi y
a todos mis amigos
Dalton Noboa M.

A mi esposa Norma,
quien me impulsó
desde el inicio.
Ernesto Murrieta F.

INDICE GENERAL

CAPITULO 1

1 Introducción

1.1. Antecedentes

Cuando hablamos de seguridad de información, debemos considerar a la información como un activo crítico de las organizaciones y como tal se debe preservar su integridad, confidencialidad y disponibilidad. No es posible eliminar por completo los riesgos, sin embargo es posible reducirlos mediante controles de protección contra amenazas y vulnerabilidades.

En estos tiempos, es importante que las empresas cuenten con un Sistema de Gestión de Seguridad de Información (SGSI), que les facilite el establecer, implementar, operar, monitorear y mantener la seguridad de la información de sus empresas, es por tal razón que la Escuela Superior Politécnica del Litoral como institución de prestigio a nivel nacional e internacional, no puede dejar de lado este tema.

ESPOL no está libre de sufrir ataques informáticos, para citar un ejemplo, mencionamos la información enviada en un correo electrónico a toda la institución, donde se reporta un ataque informático a una de las unidades que posee ESPOL.


CENTRO DE PROMOCION Y EMPLEO DE LA ESPOL - Mensaje (HTML)

Archivo Edición Ver Insertar Formato Herramientas Acciones ?

Responder | Responder a todos | Reenviar

De: CEPROEM [ceproem@espol.edu.ec] Enviado el: Jueves 05/01/2006 14:08
Para: ceproem@espol.edu.ec
CC:
Asunto: CENTRO DE PROMOCION Y EMPLEO DE LA ESPOL

CENTRO DE PROMOCION Y EMPLEO DE LA ESPOL

El CEPROEM, quien tiene a su cargo la realización de los Encuentros Laborales, pide mil disculpas por las molestias ocasionadas últimamente en los registros de la página web para la participación en el noveno Encuentro Laboral 2006.
Lamentablemente este inconveniente surgió porque el servidor fue hakeado aproximadamente hace 2 semanas por personas extranjeras, ocasionando la pérdida parcial de la información.
Agradecemos su compresión y pedimos confirmar si sus datos están ingresados en la base de datos, caso contrario deberán actualizar su información.

El presente proyecto de graduación del Diplomado de Auditoria Informática tiene como objetivo el diseñar las bases para la implementación de un Sistema de Gestión de la Seguridad de la Información.

1.2. Introducción a la seguridad de la información

Hoy en día la información es un recurso que, como el resto de los importantes activos comerciales, tiene valor para una organización y por consiguiente debe ser debidamente protegida. La seguridad de la información protege ésta de una amplia gama de amenazas, fraudes asistidos por computadora, espionaje, sabotaje, vandalismo, incendios o inundaciones, daños provocados por virus informáticos, hacking, etc., a fin de garantizar la continuidad comercial, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades.

La información se puede presentar o existir en varias formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

La seguridad de la información se define como la preservación de las siguientes características:

Confidencialidad de la información: La información que se intercambian entre individuos y empresas no siempre deberá ser conocida por todo el mundo. Mucha de la información generada por las personas se destina a un grupo específico de individuos, y muchas veces a una única persona. Eso significa que estos datos deberán ser conocidos solo por un grupo controlado de personas.

Integridad de la información: Una información integra es una información que no ha sido alterada de forma indebida o no autorizada. Para que la información se pueda utilizar, deberá estar integrada. Cuando ocurre una alteración no autorizada de la información, quiere decir que la información ha perdido su integridad.

Disponibilidad: Para que una información se pueda utilizar, deberá estar disponible. Se refiere a la disponibilidad de la información y de toda la estructura física y tecnológica que permita el acceso, transito y almacenamiento. La disponibilidad de la información permite que:

- Se utilice cuando sea necesario.
- Que este al alcance de sus usuarios y destinatarios.

- Se pueda accederla en el momento en que necesiten utilizarla.

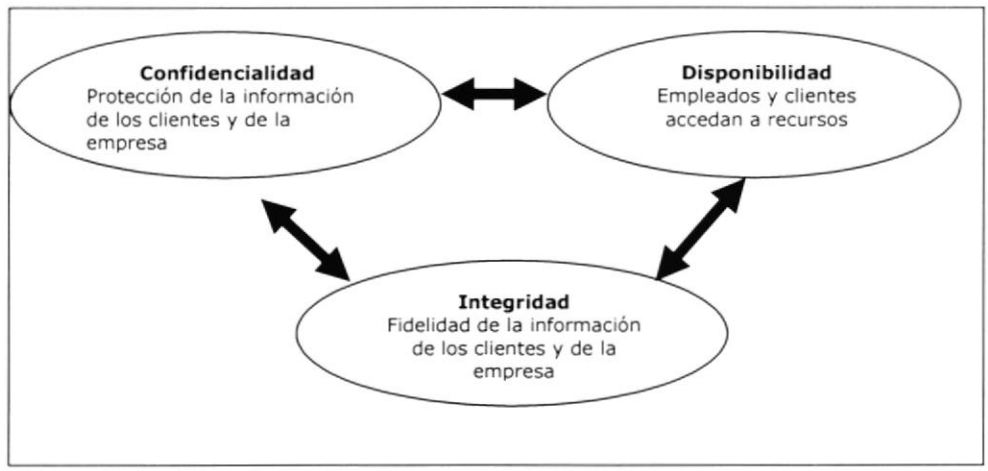


Figura 1.1. Características de la información

¿Una pregunta que a veces nos realizamos es, Por qué es necesaria la seguridad de la información?

Como se ha comentado la información, los procesos, sistemas y redes que le brindan apoyo constituyen importantes recursos de la empresa. Si se logra asegurar que la información posea las tres características: confidencialidad, integridad y disponibilidad, esto puede generar o mantener una ventaja competitiva, el flujo de fondos, la rentabilidad, el cumplimiento de las leyes y la imagen comercial. Es importante mencionar que el éxito de una empresa dependerá entre otras cosas de la calidad de la información que genera y gestiona.

Por todo lo antes mencionado se hace necesaria la seguridad de la información, la cual se logra implementando un conjunto adecuado de controles, que abarcas políticas, prácticas, procedimientos, estructuras organizacionales y funciones del software y hardware.

La identificación de los controles que deben implementarse requiere una cuidadosa planificación y atención a todos los detalles. Una vez identificados los requerimientos de seguridad, deben seleccionarse e implementarse controles para garantizar que los riesgos sean reducidos a un nivel aceptable. Los controles además deben de ser seleccionados teniéndose en cuenta el costo de implementación en relación con los riesgos a reducir y las pérdidas que podrían producirse de tener lugar una violación de la seguridad. También deben tenerse en cuenta los factores no monetarios, como el daño en la reputación.

La administración de la seguridad de la información, exige, como mínimo, la participación de todos los empleados de la organización.

1.3. Entorno organizacional CSI-ESPOL

1.3.1 Organización Institucional

La Escuela Superior Politécnica del Litoral es una persona jurídica de derecho público, autónoma en lo académico, científico, técnico, administrativo y económico, sin más restricciones que las señaladas en la Constitución y las leyes.

Tiene carácter unitario e indivisible y se regirá por las disposiciones de la Ley de Universidades y Escuelas Politécnicas, por las del Decreto Ejecutivo No. 1664 del 29 de octubre de 1958, mediante el cual se creó la Escuela, en lo que fueren aplicables, y por el presente Estatuto y sus reglamentos.

Son sus funciones principales, la formación profesional y técnica, la investigación científica, la prestación de servicios, el planteamiento de soluciones para los problemas del país en los campos y áreas relacionadas con su vida académica; el desarrollo y difusión de la cultura nacional; y, la participación en las acciones que contribuyan a crear una nueva y más justa sociedad ecuatoriana.

ESPOL cuenta con 233 profesores con nombramiento divididos en las siguientes categorías:

- Profesores Principales 146
- Profesores Agregados 42
- Profesores Auxiliares 45

Además, cuenta con 26 profesores contratados bajo contratos con relación de dependencia, también cuenta con 612 profesores contratados bajo la modalidad de contratos por horas de clase dictadas. En el Área Administrativa cuenta con 315 empleados con nombramiento.

Las actividades fundamentales se desarrollan en 6 campus: Gustavo Galindo, Las Peñas, CENAIM, Santa Elena, Daule y Samborondón.

El campus Gustavo Galindo tiene una extensión de 724 hectáreas, está ubicado en el Km. 30.5 de la vía Perimetral, es donde se encuentra localizada la administración central y de la mayoría de las carreras de pregrado que oferta ESPOL. Su moderna infraestructura es el resultado del Plan de Desarrollo 1983-1992 que se financió con el préstamo BID-ESPOL II.

El campus Las Peñas tiene una extensión de 2.5 hectáreas, está ubicado al pie del más antiguo barrio de la ciudad. En este campus se realiza una amplia y diversificada vida académica que atiende

tanto la formación de pregrado y postgrado, cuanto la actualización y mejoramiento profesional.

El CENAIM, está ubicado en San Pedro de Manglaralto, en la ruta del Sol de la Península de Santa Elena, su esfuerzo académico está orientado a potenciar la capacidad productiva del sector acuícola ecuatoriano y ser un espacio académico internacional.

El campus Santa Elena está ubicado en la cabecera del cantón del mismo nombre, oferta carreras vinculadas a las Tecnologías Pesquera y Computacional.

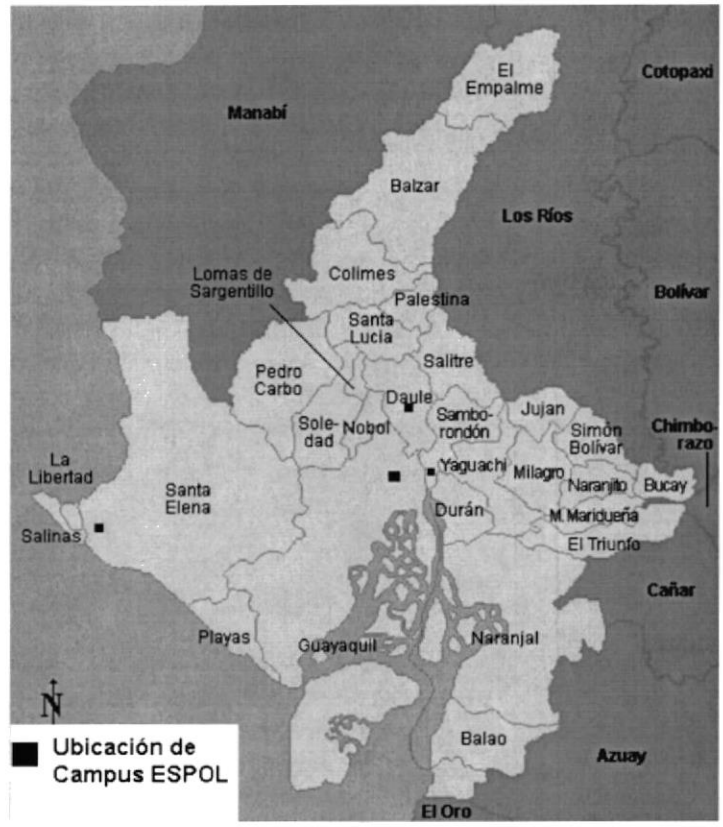


Figura 1.2 Ubicación de Campus de ESPOL

El campus Daule está ubicado a 46 Km. al norte de Guayaquil, trabaja específicamente en el campo de la agricultura, formando bachilleres y tecnólogos, en estrecha conexión con el sector productivo, especialmente arrocero.

El campus Samborondón ubicado en la entrada del cantón del mismo nombre, oferta las carreras de Secretariado Ejecutivo y Programación de Sistemas. Este campus brinda carreras pertenecientes al Programa de Tecnología de Computación, que tiene su sede en el campus Peñas.

1.3.2 Misión

La Misión de ESPOL es: "Formar profesionales de excelencia, líderes emprendedores, con sólidos valores morales y éticos, que contribuyan al desarrollo del país para mejorarlo en lo social, económico, político y ambiental. Hacer Investigación, Transferencia y Extensión de calidad para servir a la sociedad."

1.3.3 Visión

"Ser líder y referente de la Educación Superior de América Latina."

1.3.4 Valores

Compromiso con la excelencia académica: La excelencia académica es una meta superior, permanente y cotidiana. Es la condición básica para que ESPOL cumpla la finalidad y los objetivos que la Constitución y la Ley determinan.

Mística de Trabajo: Trabajar y cumplir para que ESPOL refuerce y amplíe su prestigio y liderazgo.

Responsabilidad: Cumplir con calidad y a tiempo, todas las tareas institucionales. Cumplir sus compromisos y asumir las consecuencias de las acciones y omisiones.

Honestidad: Manejar los asuntos personales e institucionales con integridad y probidad, basados en la práctica de valores.

Solidaridad: entre los miembros de la comunidad universitaria y con la colectividad en general.

Imparcialidad: Independencia en las decisiones institucionales. Mantener relaciones con nuestros aliados estratégicos, entre pares, y la cooperación recíproca, con la finalidad de buscar la verdad y el desarrollo integral del Ecuador.

1.3.5 Gobierno de ESPOL

La Escuela Superior Politécnica del Litoral es una comunidad que está constituida por profesores, alumnos y trabajadores. El gobierno de ESPOL es ejercido jerárquicamente por los siguientes organismos y autoridades.

Figura 1.3 Foto de autoridades de ESPOL

A nivel Institucional

- La Asamblea Politécnica
- El Consejo Politécnico
- El Rector
- El Vicerrector General
- El Vicerrector Administrativo-Financiero
- El Vicerrector de Asuntos Estudiantiles y Bienestar.

A nivel de Ingenierías y de Ciencias

- La Junta de Facultad y de Instituto de Ciencias
- El Consejo Directivo de Facultad y de Instituto de Ciencias
- El Decano de Facultad y Director de Instituto de Ciencias
- El Subdecano de Facultad y Subdirector de Instituto de Ciencias

A nivel de Tecnología

- La Junta del Instituto de Tecnologías
- El Director del Instituto de Tecnologías
- El Subdirector del Instituto de Tecnología
- La Junta Académica de Programa
- El Coordinador de Programa de Tecnología

1.3.6 Estructura Organizacional

ESPOL luego de sus 45 años de vida, para poder realizar sus actividades fundamentales, y operar los 5 campus, ha adoptado una estructura organizacional corporativa, con unidades estratégicas conformadas por una estructura académica administrativa, donde opera el gobierno y administración central, fundaciones y empresas, como se muestra en el siguiente gráfico.

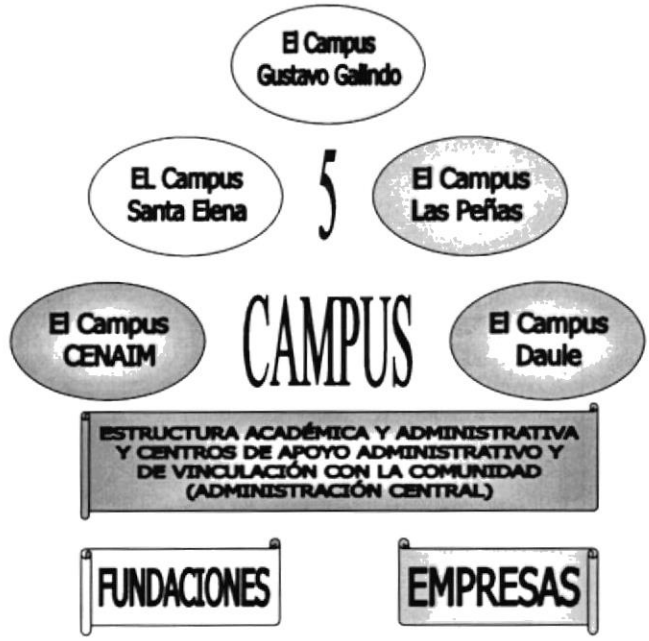


Figura 1.4 Estructura corporativa de ESPOL

La primera unidad estratégica está compuesta por las unidades académicas, las unidades de apoyo y de gestión y los centros de apoyo y de vinculación con la comunidad, y, todas ellas que se encuentran dentro de la estructura de la administración central.

La segunda unidad estratégica la constituyen las fundaciones, que son entes descentralizados que se rigen por su propio estatuto y sus directorios están conformados por autoridades de ESPOL y miembros del Consejo Politécnico y, otras fundaciones como el CENAIM –ESPOL y Fundación ESPOL 50 años, cuyos directorios están conformados por miembros del Consejo Politécnico y por empresarios pertenecientes al sector productivo.

La fundación CENAIM-ESPOL tiene sus oficinas en el Campus Gustavo Galindo y utiliza el backbone de ESPOL. Adicional, posee una estación científica marina en la comunidad de San Pedro, del cantón Santa Elena, la cual posee su propia infraestructura tanto física como tecnológica.

La Fundación ESPOL 50 años tiene sede dentro del edificio principal del Campus Gustavo Galindo.

Y las empresas forman la tercera unidad estratégica. A continuación se describen las empresas de ESPOL

EMPRESA	FUNCIÓN BÁSICA
ESPOLTEL	Empresa encargada de administrar las Tecnologías de información, computación y comunicación. ESPOL posee el 100% de las acciones

Servicios de Biotecnología Compañía Anónima (CEBIOCA)	Empresa dedicada a desarrollar tecnología en el campote la biotecnología enfocada principalmente en el banano y caña de azúcar. ESPOL posee el 20% de las acciones, el resto de acciones la poseen empresarios del sector bananero y cañicultor.
TRANSESPOL	Empresa encargada de administrar el sistema de transporte de ESPOL para dar servicio a la comunidad, ESPOL posee el 100% de las acciones.
AGROSAIZA	Empresa encargada de hacer importación de materias primas, siembra, cultivo, fabricación, comercialización de productos agrícolas, especies vegetales, maquinarias, herramientas, repuestos y vehículos para el sector agropecuario y agroindustrial.
EXPOPEZA	Microempresa encargada del Manejo de Cultivos Orgánicos.

Tabla 1.1 Empresas de ESPOL

El organigrama estructural de ESPOL, vigente aprobado por el Consejo Politécnico en septiembre de 2004 se muestra en el ***ANEXO 1.- Organigrama Estructural de ESPOL.***

En el ***ANEXO 2.- Funciones básicas centros y unidades de ESPOL,*** se detallan las funciones básicas que cumplen los diferentes centros y unidades de ESPOL, entre ellos el Centro de Servicios Informáticos de ESPOL.

1.3.7 Políticas institucionales

- Trabajar con estándares internacionales para garantizar la excelencia académica.
- Ampliar los vínculos de colaboración a nivel mundial con instituciones de excelencia para fortalecer nuestras actividades académicas.
- Fortalecer los vínculos con los actores claves del Ecuador para asegurar la pertinencia del quehacer politécnico.
- Poner el adelanto tecnológico y la cultura emprendedora al servicio del desarrollo humano.
- Orientar las inversiones a favor de la excelencia académica y el bienestar politécnico.
- Promover el cultivo y práctica de los valores éticos y morales.

1.3.8 Política de Calidad (junio 2005)

a. Implantar y mantener un Sistema de Gestión de la Calidad adecuado a ESPOL, que permita satisfacer las necesidades y expectativas de los clientes, basándose en los requisitos de la norma ISO 9001:2000.

b. Llevar a cabo nuestras actividades de docencia, de investigación, de transferencia de tecnología y de extensión de calidad para servir a la sociedad, garantizando el cumplimiento de las normas legales y reglamentarias, aplicables a los productos o servicios que ofrece ESPOL.

c. Promover la mejora continua como un principio fundamental aplicable a todos los procesos de ESPOL.

d. Generar un compromiso dinámico de los Recursos Humanos de la institución, que permita mantener activo el Sistema de Gestión de la Calidad.

e. Fundamentar el Sistema de Gestión de la Calidad en la prevención de no conformidades como un medio que proporcione a los clientes, productos y servicios de calidad; por consiguiente, el personal de ESPOL, tiene la responsabilidad de informar a la Dirección, a través de los canales establecidos, cualquier situación, real o potencial, que afecte al Sistema.

1.3.9 Plan Estratégico (2003 – 2007)

Los principales objetivos contemplados en el Plan Estratégico de ESPOL 2003-2007, están agrupados en las siguientes áreas estratégicas:

- Gestión Académica
- Gestión Científica y Tecnológica
- Gestión de las Tecnologías de Información y Comunicación
- Vínculos con la comunidad
- Bienestar Politécnico
- Gestión Administrativo-Financiera
- Desarrollo de la Infraestructura Física

Adicionalmente a los objetivos establecidos en las áreas entes mencionadas ESPOL se planteó el objetivo general # 56: "Obtener la acreditación institucional de ESPOL ante el Consejo Nacional de Acreditación y Evaluación (CONEA)", el cual evalúa la calidad de todas las áreas estratégicas.

Objetivos en relación a la Gestión Académica

1. Reestructurar el sistema de admisión de las carreras de pregrado.
2. Ofertar programas específicos de inserción de los tecnólogos a las carreras de Ingeniería.
3. Ofertar programas de Licenciatura para los Tecnólogos.
4. Crear las Licenciaturas en Ciencias con mención en Educación.
5. Incrementar la oferta de Ingenierías con la actual estructura.
6. Ofertar asignaturas, carreras y programas mediante modalidad a distancia.
7. Consolidar el programa de becas en el extranjero para formar recursos humanos al más alto nivel académico.
8. Completar y modernizar la infraestructura técnica del Centro de Información Bibliotecaria, Laboratorios y Talleres.
9. Incluir en las Ingenierías la mención en Biotecnología.
10. Crear las políticas y estructuras curriculares de la era del conocimiento, para fortalecer nuestra vida académica.
11. Diseñar y ejecutar el Plan de Perfeccionamiento Docente.
12. Incrementar la oferta de programas de Postgrado en Ciencias e Ingenierías.
13. Medir, de manera objetiva, sistemática y permanente la calidad de la educación que impartimos.

Objetivos en relación a la Gestión Científica Tecnológica

14. Establecer estrategias y políticas para el fortalecimiento de la investigación científica y tecnológica.
15. Proporcionar, desarrollar y fortalecer las capacidades de investigación y su gestión en la institución.
16. Publicar los avances y resultados de los proyectos de investigación en los órganos de difusión internos y en revistas indexadas.
17. Publicar libros relevantes para la educación superior y otros ligados a la investigación y desarrollo en ESPOL.
18. Impulsar y desarrollar la creatividad para proyectos de innovación tecnológica.
19. Promover y financiar investigaciones que generen invenciones susceptibles de ser explotadas, y crear las condiciones institucionales para generar ingresos provenientes de patentes, marcas registradas y otras formas previstas en las leyes ecuatorianas.

Objetivos en relación a la Gestión de las Tecnologías de Información y Comunicación. (en adelante TICs)

20. Ofertar a todos los estudiantes, profesores y trabajadores de ESPOL, medios de acceso apropiados a las facilidades que ofrecen las TICs.

21. Propiciar las oportunidades que ofrecen las TICs, de manera que sus servicios y aplicaciones cumplan los estándares internacionales.
22. Descentralizar la responsabilidad de la planificación, adquisición, operación y mantenimiento de los recursos tecnológicos especializados, en concordancia con los estándares, políticas del uso de la TICS y los servicios de calidad que oferta ESPOL.
23. Lograr que todos los estudiantes adquieran un nivel de competencia en el uso de las TICs, apropiado para sus estudios y vocación.
24. Lograr que la planta de empleados de ESPOL mantenga un nivel de competencia en el uso de las TICs, apropiado con las actividades que desarrollan en su área.
25. Lograr que la planta docente de ESPOL mantenga un nivel de competencia en el uso apropiado de las TICs en el aula, y en la actividad académica y de investigación que desarrolla en su área.

Objetivos en relación a los Vínculos con la Comunidad

26. Crear los Centros de Transferencia y Desarrollo de Tecnologías que tengan el apoyo real de los sectores productivos.
27. Implantar el Parque Tecnológico de Guayaquil en el campus "Gustavo Galindo Velasco".
28. Crear las políticas y estructuras para desarrollar el emprendimiento e incubadoras de empresas de base tecnológica en ESPOL.
29. Liderar la prestación de servicios científico-técnicos y la capacitación de recursos humanos que requieren los sectores productivos y los organismos públicos del Ecuador.
30. Consolidar el Programa de Apoyo a la Península de Santa Elena.
31. Fortalecer la presencia editorial de ESPOL.
32. Ejecutar proyectos de colaboración recíproca con sectores productivos.
33. Medir, de manera objetiva, sistemática y permanente, la calidad de la prestación de servicios y de los diferentes componentes de la vinculación con la comunidad, e introducir esa tarea como rutinaria en la vida de ESPOL.

Objetivos en relación al Bienestar Politécnico

34. Garantizar remuneraciones competitivas para profesores y trabajadores.
35. Consolidar el Fondo de Jubilación.
36. Disminuir la tasa de deserción estudiantil causada por la falta de financiamiento para estudios.
37. Reducir los índices de estudiantes que entran en período de prueba.

38. Ampliar la cobertura de las exoneraciones y becas para premiar a los estudiantes de buen rendimiento académico y bajos recursos económicos, así como a los estudiantes que alcancen éxitos deportivos, académicos y culturales y a los que participen en Programas de Vínculos con la Colectividad.
39. Crear el Seguro Estudiantil de Salud.
40. Mejorar la calidad de los servicios de transporte, salud y comedores.
41. Fomentar y diversificar la práctica del deporte.
42. Fomentar y diversificar la práctica del arte y la cultura.
43. Ejecutar el Programa de Readecuación Física y Tecnológica de las aulas.
44. Favorecer la inserción de los profesionales politécnicos en el mercado laboral nacional e internacional.

Objetivos en relación a la Gestión Administrativo Financiera

45. Redefinir la estructura institucional.
46. Diseñar, implementar y mantener un sistema de gestión de la calidad que cumpla con los requisitos de la norma ISO 9001:2000 y mejorar continuamente su eficacia.
47. Mejorar la calidad del servicio administrativo-financiero para contribuir al desarrollo académico y optimizar la atención a los usuarios de ESPOL.
48. Constituir un fondo de operación que garantice liquidez.
49. Manejar y usar la información como elemento clave de la gestión.
50. Formular y ejecutar el Programa de Identidad e Imagen Corporativas.
51. Medir, de manera objetiva, sistemática y permanente, la calidad de la gestión administrativa, financiera y los servicios de bienestar politécnico y estudiantil, e introducir esa tarea como rutinaria en la vida institucional.

Objetivos en relación a la Infraestructura Física

52. Asegurar el desarrollo armónico del campus "Gustavo Galindo Velasco" y preservar su integridad.
53. Transformar el campus "Las Peñas" en un complejo académico, cultural, urbanístico y de servicios.
54. Realizar las adecuaciones físicas en el campus "Santa Elena".
55. Ejecutar las adecuaciones físicas que requiere el campus "Daule".

El Plan Estratégico se encuentra descrito en su totalidad en el ***ANEXO 3.- Plan Estratégico ESPOL 2004-2007***.

1.4. Centro de Servicios Informáticos (CSI)

La función básica del CSI es administrar el sistema de información de ESPOL tanto académico, administrativo y financiero.

1.4.1 Visión

Ser el Centro del Conocimiento de la Escuela Politécnica, con la infraestructura de Comunicación y servicios que la comunidad requiere.

1.4.2 Misión

Proveer a la Alta Dirección el acceso a los principales indicadores de gestión de la Institución, a través de una infraestructura de información y comunicación corporativa, que permitan mantener procesos que maximicen el ingreso.

1.4.3 Estructura Organizacional

De acuerdo al reglamento de creación de centros, esta unidad estará conformada por:

- Consejo Directivo, presidido por el Rector o su delegado, e integrado por dos vocales, los mismos que deberían ser dos profesores de ESPOL, que no formen parte del Consejo Politécnico.
- Director de la Unidad designado por el Rector.
- El equipo técnico que apruebe el Consejo Directivo.

1.4.4 Responsabilidades del Consejo Directivo

- Alinear las políticas y acciones con la visión, misión, políticas y planificación de ESPOL.
- Aprobar los planes operativos anuales.
- Supervisar y evaluar la gestión del Director.
- Hacer recomendaciones al Consejo Politécnico en relación con el desarrollo del Centro.
- Conocer los informes que presenta el Director y ponerlos en consideración del Consejo Politécnico.
- Aprobar el instructivo de Gestión del Centro.
- Todos los aspectos operativos del Centro.
- Los demás aspectos no previstos en estos lineamientos, serán definidos por el Rector.

1.4.5 Responsabilidades de la Unidad

- Elaborar los planes operativos anuales y presentarlos al Consejo Directivo.
- Coordinar las áreas tecnológicas que apoyen a las áreas administrativas, financiera y académica de ESPOL a nivel de todos sus Campus.

- Mantener la innovación continua de los servicios que ofrece.
- Proveer información corporativa a todos los usuarios que necesitan tomar decisiones y estrategias, para una eficaz y eficiente Gestión Institucional.
- Instalar soluciones que integren en una Red de Información Corporativa, las soluciones heterogéneas de hardware, software y comunicaciones.
- Contribuir en la formulación de las políticas de desarrollo de las Tecnologías de Información en los campus de ESPOL, en concordancia con las políticas institucionales.
- Aplicar las políticas de desarrollo y uso de las Tecnologías de Información.
- Crear y mantener una base de datos institucional.

1.4.6 Funciones de la Unidad

- Estudio, administración, e implementación de nuevas tecnologías para ofrecer nuevos servicios a ESPOL.
- Interconexión, manejo y control de los diferentes Campus que posee la universidad.
- Gestión, control, manejo y acceso a Internet de todos los Campus de ESPOL.
- Mantener el inventario de software y hardware en todas las unidades académicas, administrativas y de apoyo de ESPOL.
- Soporte tecnológico para la planificación y administración del licenciamiento de software adquirido a terceros, a nivel institucional.
- Diseño, implementación, manejo, control e interconexión de las redes de datos existentes y de nuevas redes que se enlacen al Backbone del Campus Gustavo Galindo o que se instalen en los diferentes Campus de ESPOL.
- Coordinación con los administradores de laboratorios y redes de computación para el soporte a usuarios de las diferentes unidades de ESPOL.
- Soporte a través de los administradores de laboratorios y redes de computación para la actualización, mantenimiento y mejoras del hardware y software existente en ESPOL.
- Apoyo a la gestión administrativa, financiera y académica, a través de sistemas informáticos.
- Gestión, control, manejo, mantenimiento y organización de las bases de datos de todas las áreas administrativas y educativas, que se encuentren directamente relacionadas con la administración de ESPOL.
- Soporte tecnológico principal para el desarrollo y mantenimiento de los servicios de gobierno electrónico
- Desarrollo y Mantenimiento del portal de servicios de ESPOL a través del WEB.
- Difusión de todas las iniciativas tecnológicas a nivel de los Campus de ESPOL.
- Las demás que acordare el Rector.

1.4.7 Servicios ofrecidos por el CSI

Actualmente CSI ofrece los siguientes servicios:

- Desarrollo de soluciones informáticas para la Gestión Administrativa – Financiera y Académica de ESPOL.
- Creación de cuentas electrónicas.
- Correo electrónico.
- Asesoría en Adquisición de Equipos de Computación y Telecomunicaciones.
- Diseño de Redes.
- Web Hosting (Alojamiento de páginas Web).
- Creación de Dominios (_____.espol.edu.ec).
- Soporte Técnico a Usuarios.

1.4.8 Principales soluciones informáticas

Aplicaciones / Servicios	Usuario	Responsable del desarrollo/ mantenimiento de la aplicación	Software de desarrollo	Base de datos	Información obtenida de
Administrativo-Financiero	Unidad Financiera y Personal	CSI	IBM Visual Age Smalltalk	IBM DB2	Base de Datos Financiera
Nóminas	Depto de Personal	CSI	IBM Visual Age Smalltalk	IBM DB2	Base de Datos Roles de Pago
Académico – Pregrado	CRECE, estudiantes, Unidades Académicas, VG	CSI	IBM Visual Age Smalltalk	IBM DB2	Base de Datos Académica
Académico-Sistema de Audiorespuesta	Estudiantes	CSI a través de un software adquirido a EQUIS	MS Visual Basic	IBM DB2	Base de Datos Académica
Académico-registros en línea	Estudiantes	CSI	MS .net	IBM DB2	Base de Datos Académica
Académico-Admisiones	Oficina de Ingreso	CSI	Visual Basic	SQL Server	Base de Datos propia de la unidad
Académico-kiosco electrónico	Estudiantes	CTI	Visual Basic	SQL Server	Base de Datos Académica
Académico-Postgrado	ESPAE	ESPAE	Visual Basic	SQL Server	Base de Datos propia de la unidad
Académico-exalumnos	CEPROEM	CEPROEM	Software libre (PHP)	SQL Server	Base de Datos propia de la unidad
Académico-evaluación de profesores	CENACAD	CISE	Software libre (PHP)	MySQL	Base de Datos propia de la unidad

Académico-Becarios	Relaciones Externas	Contrato a tercero. Proyecto en desarrollo	MS .net	IBM DB2	Base de Datos propia de la unidad
Sistema de Información Bibliotecaria	Biblioteca	Personal contratado en Biblioteca	Visual Basic	IBM DB2	Base de Datos propia de la unidad

Tabla 1.2 Soluciones informáticas del CSI

Nota: Los sistemas no desarrollados por CSI alimentan sus bases de datos con información que provee el CSI en sus instalaciones del Campus Gustavo Galindo en Guayaquil a través de archivos planos, que son generados cada semestre.

Dos de las principales aplicaciones desarrolladas por CSI que aportan un importantísimo valor para ESPOL son el Sistema Financiero y el Sistema Académico, la descripción de los mismos se detalla en el ***ANEXO 5.- Descripción de Sistemas Financiero y Académico ESPOL***.

1.4.9 Otros Servicios

CSI también provee de los siguientes servicios:

- Inventario de Hardware.- Presenta el inventario de Hardware (ver ***ANEXO 6.- Inventario de hardware ESPOL***).
- Licencias de software.- Presenta la lista de los software registrados legalmente por la institución. (ver ***ANEXO 7.- Inventario de software ESPOL***).
- Documentos y formularios.- Se describe los documentos y formularios que son utilizados en las distintas tramites administrativos dentro de ESPOL. (ver ***ANEXO 8.- Documentos y formularios***).
- Audioespol.- AUDIOESPOL es un servicio de Respuesta por voz que permite a estudiantes, profesores, proveedores y público en general realizar consultas desde cualquier lugar por medio del sistema telefónico convencional.
- Guía de adquisición de equipos.- Se describe una guía de adquisición para equipos informáticos dentro de ESPOL.
- Índice de Manuales.- A través de este servicio, usted podrá investigar y aprender sobre el uso de aplicaciones y software que se usa en ESPOL (ver ***ANEXO 9.- Índice de manuales***).
- Características de computadores personales.- Describe las principales características de una computadora personal dentro de ESPOL.

1.4.10 Organigrama del CSI

Ver ***ANEXO 10.- Organigrama CSI –ESPOL.***

En el ***ANEXO 11.- Funciones y responsabilidades del personal del CSI,*** se describen las funciones y responsabilidades de los puestos señalados en el ***ANEXO 10.- Organigrama CSI –ESPOL***.

1.5. Estadísticas relacionadas con la seguridad de la información.

Una definición valida de lo que podríamos definir como "Delitos Informáticos" se puede decir de: "Todas aquellas faltas contra la ley, la moral, los principios o las buenas costumbres; que se realicen o ejecuten haciendo uso de herramientas tecnológicas".

Si bien es cierto existen todavía mucho camino por recorrer en el aspecto legal en cuanto a la protección contra posibles acciones que perjudiquen a las personas naturales o jurídicas mediante el uso de tecnología, el objetivo del presente capitulo es identificar lo que ha sucedido, ha sido identificado y tipificado como Delito Informático; por lo tanto se presentara a continuación la información obtenida de diversas fuentes consultadas en la realización del presente trabajo y que ayudan a explicar las tendencias delictivas que con la incorporación de nuevos servicios tecnológicos y herramientas que desde el momento de su creación fueron implementados para mejorar y agilizar procesos, pero que si no tenemos en cuenta los riesgos potenciales de su uso podrían darnos serios dolores de cabeza.

Un estudio realizado por: CSI/FBI Computer Crime and Security Survey[1], para las estadísticas del año 2004 aplicado a 494 personas relacionadas a actividades de seguridad computacional de varios tipos de organizaciones de los Estados Unidos; la ***figura 1.5*** muestra los porcentajes por sector en la industria de las demandas realizadas por la empresas sobre actividades relacionadas a delitos relacionados contra la seguridad de sus sistemas, robo de información o hardware, fraude financiero, entre otros; la clasificación y los porcentajes fueron realizadas de un total de 486 denuncias receptadas por el FBI durante el 2004.

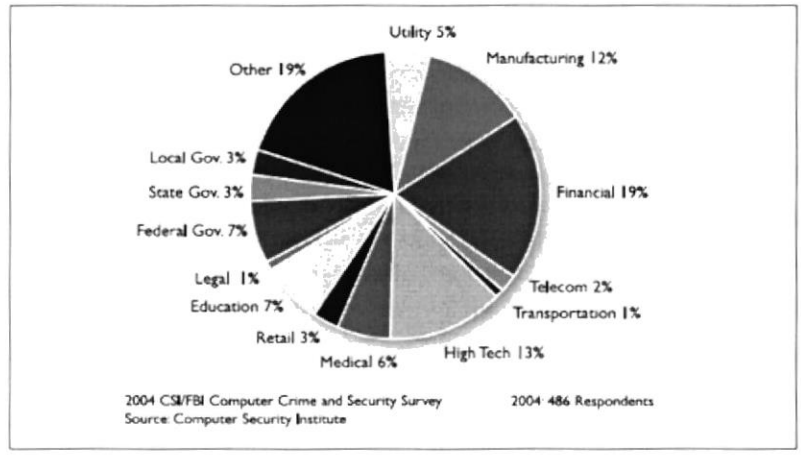


Figura 1.5 Demandas por sector de industria

[1] *CSI/FBI Computer Crime and Security Survey-2004.*
http://gocsi.com/forms/fbi/csi_fbi_survey.jhtml

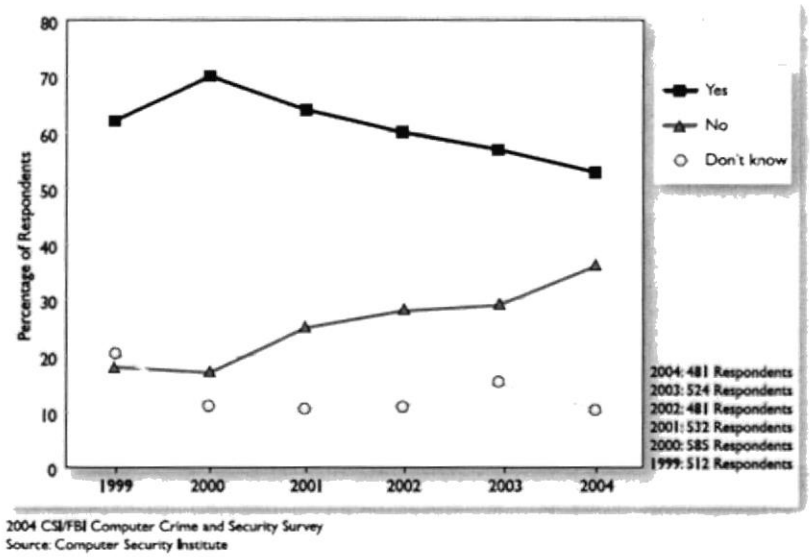


Figura 1.6 Uso no autorizado de sistemas de computo en los últimos 12 meses

La ***figura 1.6*** muestra las tendencias en las demandas registradas contra ataques (exitosos), donde se resalta que cada vez mas las organizaciones se reportan con menor frecuencia los ataques debido a varias razones entre ellas la mala publicidad que ocasiona el conocimiento público de dichos ataques.

La ***figura 1.7*** muestra los diferentes tipos de ataques o mal uso registrados en los 12 meses del 2004 agrupados en 10 categorías. El total de demandas registradas en los Estados Unidos de Norte América fue 481.

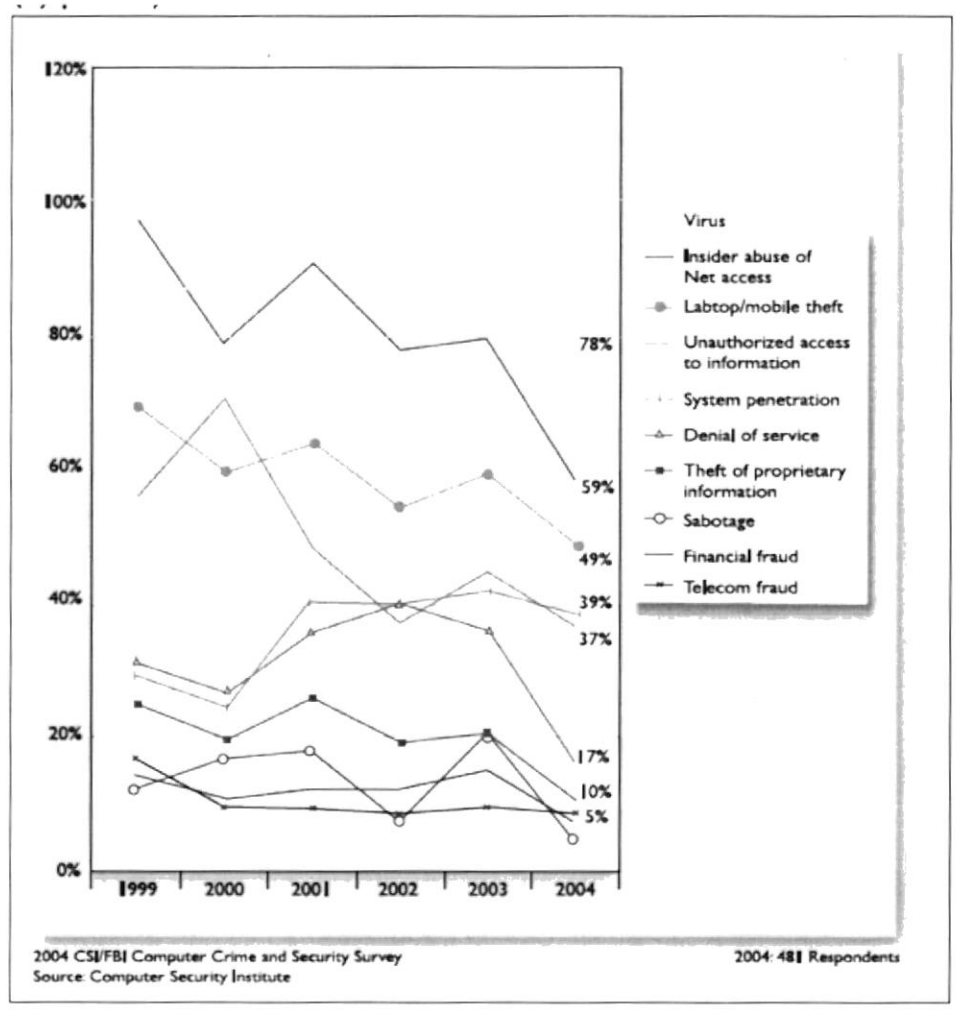


Figura 1.7 Tipos de ataques o mal uso detectados en el 2004

La ***figura 1.8*** muestra los montos para los diferentes tipos de ataques totalizados en los 12 meses del 2004 agrupados en las 10 categorías descritas en la ***figura 1.7***.

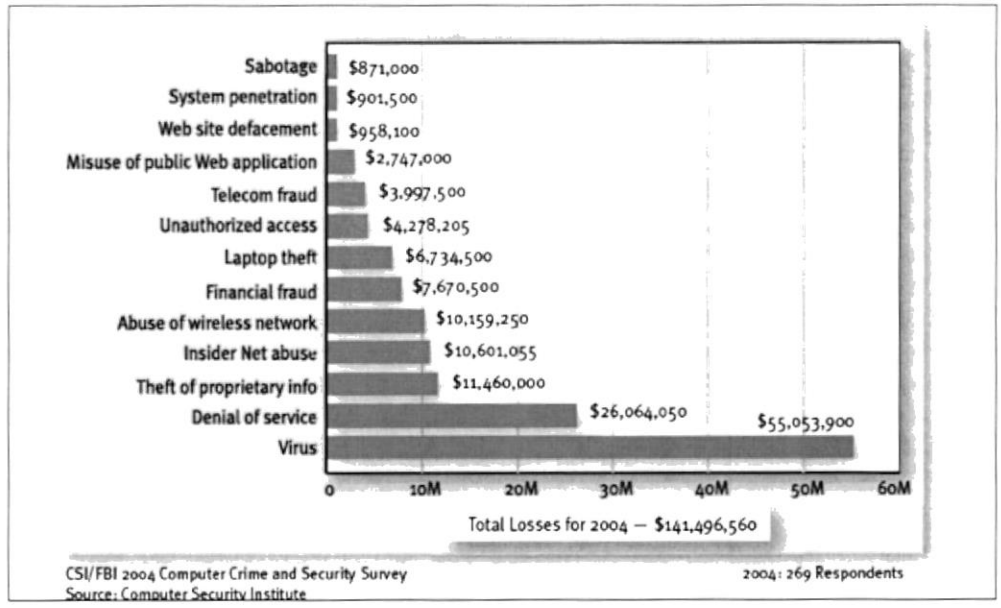


Figura 1.8 Monto de pérdidas en dólares por tipo

Si tenemos claro que el análisis anterior fue realizado para el año 2004, debemos aclarar que el alcance del mismo fue el territorio nacional de los Estados Unidos de Norte América, ya que no se han publicado trabajos de este tipo para el ámbito nacional del Ecuador. Seria muy interesante poder contar con este tipo de información para poder observar la evolución del crimen en el medio en el que trabajamos y desarrollamos nuestras actividades; pero debemos esperar la iniciativa y preocupación que se pueda presentar a los entes como el Congreso Nacional en cuanto a la tipificación y creación de leyes como de la Policía Nacional para dar un tratamiento especial a estos casos y llevar a cabo actividades que permitan preparar el terreno y estar listos a enfrentar la delincuencia 'sofisticada' y 'tecnificada' con la capacidad de disponer de recursos y medios para tipificar y crear sanciones para estos delitos, disponer especialistas que hagan el seguimiento de los mismos e informar a las personas sobre casos comunes y prevención que se deba tener para evitar ser victima de alguno de estos tipos de fraude. Teniendo en cuenta siempre que a medida que cambia la tecnología cambia la forma en que esta puede ser usada como herramienta delictiva.

ESPOL como una entidad que soporta una gran cantidad de sus procesos internos como registros, ingresos de notas, cobros de valores, pago a proveedores; con sistemas de información y tecnología en general, dentro de su estructura funcional y operativa posee vulnerabilidades, dichas vulnerabilidades como falta de segregación en las funciones, falta de controles en los procesos, desconocimiento de responsabilidades sobre la información, entre otros podrían ser explotados en cierto momento por algún agente externo o interno, de manera premeditada o por casualidad; de tal forma que se tendría un como resultado que medir el impacto de

dicho 'crimen' y el tiempo en que el mismo fue detectado ya que no podríamos asegurar que todo delito se detecta.

Por lo tanto debe considerarse importante crear o fortalecer el ambiente de control interno sobre el que operan los sistemas y se desarrollan lo procesos, asegurar la infraestructura para proteger en contra de ataques externos y concienciar a los usuarios sobre la importancia de la seguridad en el manejo general de la información sin importar el medio que contenga a la misma.

CAPITULO 2

2 Sistemas de Gestión de la Seguridad de la Información

2.1 Estándares relacionados a la Seguridad de la Información

A nivel mundial existen diferentes organismos relacionados con temas sobre la seguridad de la información, podemos mencionar los siguientes:

- IT Governance Institute and Information Systems and Audit Control Association - ISACA: METODOLOGIA COBIT.
- British Standards Institute: BS 7799-1, BS 7799-2.
- International Standards Organization: ISO 17799:2000, ISO 17799:2005, ISO 27001:2005.
- Departamento de Defensa de USA: Orange Book, Common Criteria
- Sans Institute
- Sarbanes Oxley Act, HIPAA Act a nivel de legislación

2.1.1 Information Systems and Audit Control Association – ISACA

La *Information Systems Audit and Control Association* (Asociación de Auditoria y Control de Sistemas de Información, o ISACA) es una asociación de profesionales y universitarios que se dedican a la práctica y al estudio de la auditoria, el control y la seguridad informática.

ISACA posee su metodología llamada COBIT (*(Control Objetives Information Technologies) (Objetivos de Control para la Información y Tecnologías) la cual se enfoca a la seguridad de la información.*

COBIT, basa su estándar de 34 procesos u Objetivos de Control en cuatro dominios perfectamente definidos que son:

- Planeamiento y Organización
- Adquisición e Implementación
- Entrega y Soporte
- Monitoreo

Figura 2.1 Logo de la metodología COBIT

2.1.2 British Standards Institute

Es parte del grupo global BSI y es el representa el organismo nacional de estándares de Reino Unido. Desarrolla estándares y soluciones de estandarización orientadas a las necesidades de los negocios y de la sociedad.

Existe el estándar BS-779 que consta de dos partes:
BS-7799 Parte 1 – Guía de mejores prácticas
BS-7799 Parte 2 – Requerimientos para un Sistema de Gestión de la Seguridad Informática (certificable)

Figura 2.2 Logo de la British Estándar Institute

2.1.3 Departamento de Defensa de USA: Orange Book / Common Criteria

El departamento de Defensa de Estados Unidos de Norte América ha publicado desde 1983 su *Trusted Computer System Evaluation Criteria,* mejor conocido como Orange Book y se considera como estándar para la seguridad de la computación el día de hoy y ha servido de base para algunos libros de seguridad de hoy.

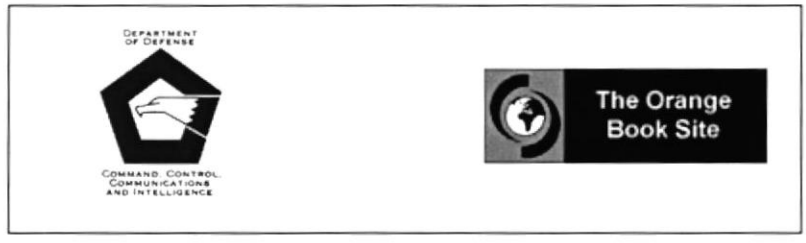


Figura 2.3 Logos del Departamento de Defensa de USA y logo del Sitio Web del Orange Book

2.1.4 Common Criteria

El Common Criteria, combina los mejores aspectos de criterios existentes para la evaluación de la seguridad de la información, sistemas y productos. Se inició en 1993 y es la alineación de un grupo de criterios existentes, como lo son el europeo (ITSEC), el de Estados Unidos (TCSEC) y el de Canadá (CTCPEC), buscando resolver las diferencias conceptuales entre las varias fuentes de criterios.

Figura 2.4 Logo de Common Criteria

2.1.5 Sans Institute

El instituto Sans es una fuente de investigación y capacitación en temas relacionado a la seguridad de la información, administración de sistemas, auditoria y seguridad en redes.

Figura 2.5 Logo de Sans Institute

2.2 International Standards Organization

La Organización de Estándares Internacionales es el organismo líder a nivel mundial en el desarrollo de estándares, los cuales especifican los requerimientos para el estado del arte de productos, servicios, procesos, materiales y sistemas, administración y prácticas organizacionales.

Existen varios estándares, sin embargo, los más conocidos son:

- ISO 9000 – orientada a Sistemas de Gestión de la Calidad
- ISO 14001 – enfocada a administración ambiental
- ISO 17799 – brinda buenas prácticas de seguridad de la información. Basada en la BS 7799 Parte 1

El alcance del presente trabajo se enfoca exclusivamente a la implementación de un Sistema de Gestión de la Seguridad Informática, los temas siguientes se relacionarán a la norma ISO 17799.

Figura 2.6 Logo del Internacional Organization for Standardization

2.3 Norma ISO 17799

El estándar ISO 17799 es un conjunto de estándares de seguridad basado en la norma BS 7799 parte 1

El alcance de ésta norma es brindar una serie de recomendaciones para la gestión de la seguridad de la información y servir de base común para el desarrollo de estándares de seguridad y poder implementar un conjunto adecuado de controles.

La última versión de la norma fue revisada y actualizada en el año 2005

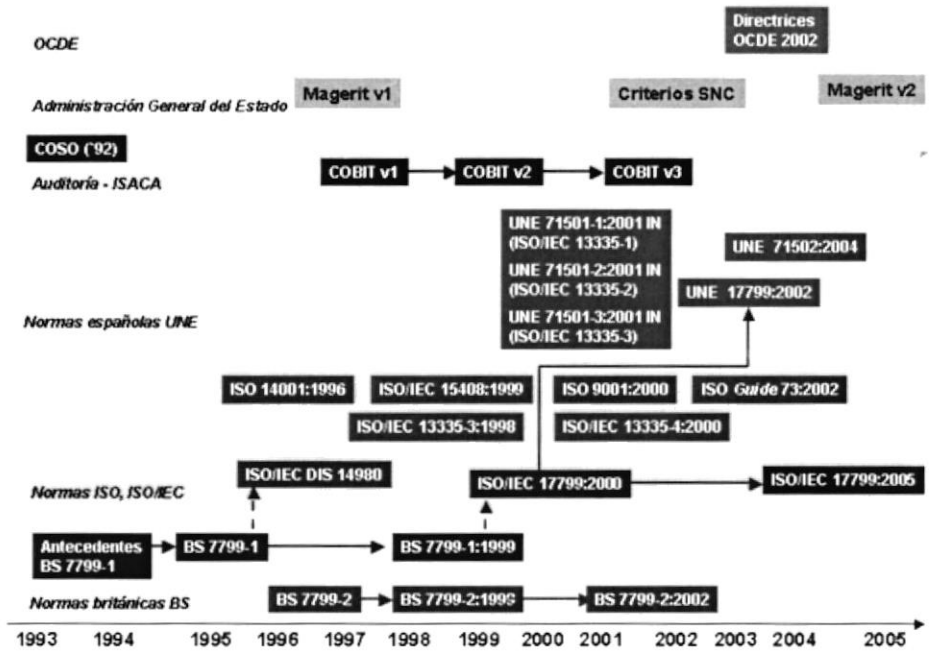


Figura 2.7 Historia de la norma ISO 17799

Se encuentra dividida en 11 partes o también llamadas Dominios los cuales son:

1. **Política de Seguridad**
   Objetivo: Proporcionar dirección y apoyo gerencial para brindar seguridad de la información.

2. **Organización de la Seguridad de la Información**
   Objetivo: Administrar la seguridad de la información dentro de la organización. Debe establecerse un marco gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

3. **Administración de activos**
   Objetivo: Mantener una adecuada protección de los activos de la organización.

4. **Seguridad del Recurso Humano**
   Objetivo: Reducir los riesgos de error humano, robo, fraude o uso inadecuado de instalaciones.

5. **Seguridad Física y Ambiental**
   Objetivo: Impedir accesos no autorizados, daños e interferencia a las sedes e información de la empresa.

6. **Administración de las Comunicaciones y Operación**
   Objetivo: Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.

7. **Control de accesos**
   Objetivo: Controlar el acceso de información.

8. **Adquisición, desarrollo y mantenimiento de sistemas de información**
   Objetivo: Asegurar que la seguridad es incorporada a los sistemas de información.

9. **Administración de incidentes de seguridad de la información**
   Objetivo: Asegurarse que la seguridad de la información es comunicada en una forma que permita que una acción correctiva sea tomada en un tiempo adecuado.

10. **Administración de la continuidad del negocio**
    Objetivo: Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos críticos de los negocios de los efectos de fallas significativas o desastres.

11. **Cumplimiento**
    Objetivo: Impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

<table>
<tr><td colspan="4">Política de Seguridad</td></tr>
<tr><td colspan="4">Organización de la Seguridad de la Información</td></tr>
<tr><td colspan="4">Administración de activos</td></tr>
<tr><td>Seguridad del Recurso Humano</td><td>Seguridad Física y Ambiental</td><td>Administración de las Comunicaciones y Operación</td><td rowspan="2">Adquisición, desarrollo y mantenimiento de sistemas de información</td></tr>
<tr><td colspan="3">Control de accesos</td></tr>
<tr><td colspan="4">Administración de incidentes de seguridad de la información</td></tr>
<tr><td colspan="4">Administración de la continuidad del negocio</td></tr>
<tr><td colspan="4">Cumplimiento</td></tr>
</table>

Tabla 2.1 Dominios de la Norma ISO 17799:2005

Cada Dominio de la norma tiene sus Objetivos de Control y a su vez, éstos tienen definidos sus respectivos controles.

La siguiente figura muestra un resumen de la norma en objetivos de control y controles.

Cláusulas de Control	Categorías Ppales de Seguridad	Controles
Areas de Control	Objetivos de Control	Controles
► 5) Política de seguridad	1	2
► 6) Organización de la seguridad de la información	2	11
► 7) Gestión de activos	2	5
► 8) Seguridad de los recursos humanos	3	9
► 9) Seguridad física y ambiental	2	13
► 10) Gestión de comunicaciones y operaciones	10	32
► 11) Control de acceso	7	25
► 12) Sistemas de información; adquisición, desarrollo y mantenimiento	6	16
► 13) Gestión de incidentes de seguridad de la información	2	5
► 14) Gestión de la continuidad del negocio	1	5
► 15) Cumplimiento	3	10
TOTAL 11	39	133

Figura 2.8 Resumen de la Norma ISO 17799:2005

Clause	Security Category	Objectives	Controls	v2000	
1	Scope	-	-	-	
2	Terms and Definitions	-	-	-	
3	Structure of the Standard	-	-	-	
4	Risk Assessment and Treatment	-	-	-	
5	Security Policy	1	2	1 – 2	Nil
6	Organising Information Security	2	11	3 – 10	-1 / +1
7	Asset Management	2	5	2 – 3	0 / +2
8	Human Resources Security	3	9	3 – 10	0 / +1
9	Physical and environmental Security	2	13	3 – 13	+1 / 0
10	Communications and Operations Management	10	32	7 – 24	+3 / +8
11	Access Control	7	25	8 – 31	-1 / -6
12	Information Systems Acquisition, Development and Maintenance	6	16	5 – 18	+1 / +2
13	**Information Security Incident Management**	2	5	0 – 0	+2 / +5
14	Business Continuity Management	1	5	1 – 5	Nil
15	Compliance	3	10	3 – 11	0 / -1
Total		39{36}	133{127}		+3 / +6

Figura 2.9 Comparación de la Norma ISO 17799:2000 vs. ISO 17799:2005

2.4 Sistemas de Gestión de la Seguridad de la Información (SGSI)

Un Sistema de Gestión implementa los procesos que permiten que una empresa realice un servicio o producto de manera confiable y en conformidad con unas especificaciones internacionales.
Las Normas ISO/UNE 17799 y UNE 71502 describen un SGSI (Sistema de Gestión de la Seguridad de la Información) aplicable a todas las organizaciones, independientemente de su tipo, tamaño o personalidad jurídica. Resulta compatible con otros sistemas de gestión empresarial, como el de Calidad, el Medioambiental o el de Prevención de Riesgos Laborales.
La ISO 17799 es un código de buenas prácticas, donde las empresas pueden encontrar los controles necesarios para gestionar la seguridad de su información.
UNE 71502 contiene las especificaciones de los Sistemas de Gestión de Seguridad de la Información que se requieren para obtener la certificación del SGSI implantado.

Está basado por el modelo utilizado por las normas ISO en general:

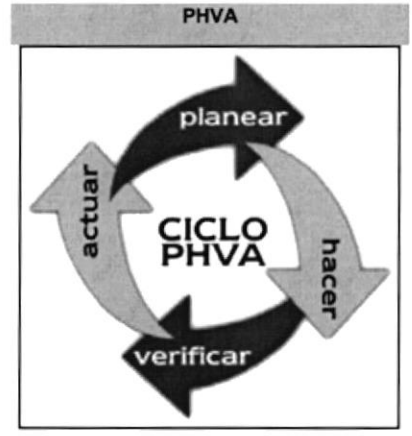


Figura 2.10 Ciclo PHVA

Planificar: Definir el SGSI
Consiste en establecer controles, políticas y procedimientos para la administración de los riesgos y mejora de la seguridad de la información.

Hacer: Implementar y operar el SGSI
Ejecutar las acciones definidas en los controles, los procesos y los procedimientos.

Verificar: Realizar el seguimiento y revisar el SGSI
Evaluar y medir el desempeño de los procesos respecto a las definiciones aprobadas e informar los resultados para la revisión.

Actuar: Mantener y mejorar el SGSI
Tomar acciones correctivas y preventivas para el logro de la mejora continua del SGSI.

2.5 Implementación de un sistema de gestión de la seguridad de la información

Para la implementación de un Sistema de Gestión de la Seguridad de la Información existen varias metodologías. Sin embargo, todas se enfocan a realizar los siguientes pasos:

1. Obtener el apoyo de la alta dirección al Sistema de Gestión de la Seguridad de la Información.

2. Definir el alcance del Sistema de Gestión de la Seguridad de la Información, considerando:
    a. Actividad de la organización
    b. Activos
    c. Tecnología
    d. Punto de vista de la alta gerencia

3. Definir la Política de la Seguridad de la Información

4. Definir una metodología para clasificar riesgos

5. Identificar y Valorar riesgos

6. Identificar y definir alternativas para el tratamiento de riesgos para:
    a. Aplicar controles
    b. Aceptar riesgos
    c. Evitar riesgos
    d. Transferir los riesgos asociados a las actividades a otras partes

7. Seleccionar objetivos de control y controles que serán implementados

8. Elaborar una Declaración de Aplicabilidad, la cual indica que controles se implementarán

9. Obtener la aprobación de:
    a. Declaración de aplicabilidad
    b. Riesgos Residuales no cubiertos

10. Formular un plan concreto y detallado para:
    a. Tratamiento de los riesgos
    b. Implementar los controles determinados
    c. Realizar programas de entrenamiento a usuarios
    d. Gestionar el Sistema de Gestión de la Seguridad de la Información
    e. Detectar y responder a los incidentes de seguridad

11. Implementar los controles

a. Controles en los procesos de usuarios
b. Controles automáticos en las tecnologías
c. Determinar la documentación de respaldo
d. Determinar los registros de respaldo

12. Realizar revisiones periódicas mediante auditorias para conocer el estado de:
    a. Los controles implementados
    b. Nuevos riesgos presentes
    c. Los riesgos residuales

13. Implementar las mejoras en el Sistema de Gestión de la Seguridad de la Información

2.6 Proceso de certificación de un Sistema de Gestión de la Seguridad de la Información

Un proceso de certificación consiste en la generación de un informe firmado por parte de un organismo externo, es decir, ajeno a la organización que define que, de acuerdo con su criterio profesional, la organización cumple o no cumple con los requerimientos establecidos en la norma.

La norma ISO 17799:2005 no es certificable, debido a que es una guía de mejores prácticas para la seguridad de la información. Al derivarse de la norma británica BS-7799 Parte 1 que no es certificable, da como conclusión que la norma ISO 17799 tampoco sea certificable.

La norma ISO 17799:2005 en su texto, da las pautas para el diseño del sistema de gestión de la seguridad informática, pero no indica como implementarlo.

La norma británica BS-7799 Parte 2 en cambio, provee de las guías necesarias para la implementación y deja de ser una guía de mejores prácticas para convertirse en una guía de requerimientos para la implementación. Ésta norma si es certificable.

En octubre del 2005, apareció la norma ISO 27001, la cual se deriva de la BS-7799 Parte 2, por lo tanto, ésta norma ISO 27001 si es certificable.

Para la implementación de un Sistema de Gestión de la seguridad de la Información, según la norma ISO 27001 se basa en 6 procesos:

1. Definir una Política de Seguridad de la Información
2. Definir el alcance del sistema de gestión de la seguridad de la información
3. Desarrollar una evaluación de los riesgos de la seguridad
4. Manejo de los riesgos identificados
5. Seleccionar los controles que serán implementados y aplicados
6. Preparar la declaración de aplicabilidad

Comparando con la metodología anterior, se observa que no existen variaciones considerables.

Para que una organización certifique su Sistema de Gestión de la Seguridad de la Información, debe demostrar que cumple con las especificaciones de la norma ISO 27001 que a su vez se basan en lo establecido en la norma ISO 17799.

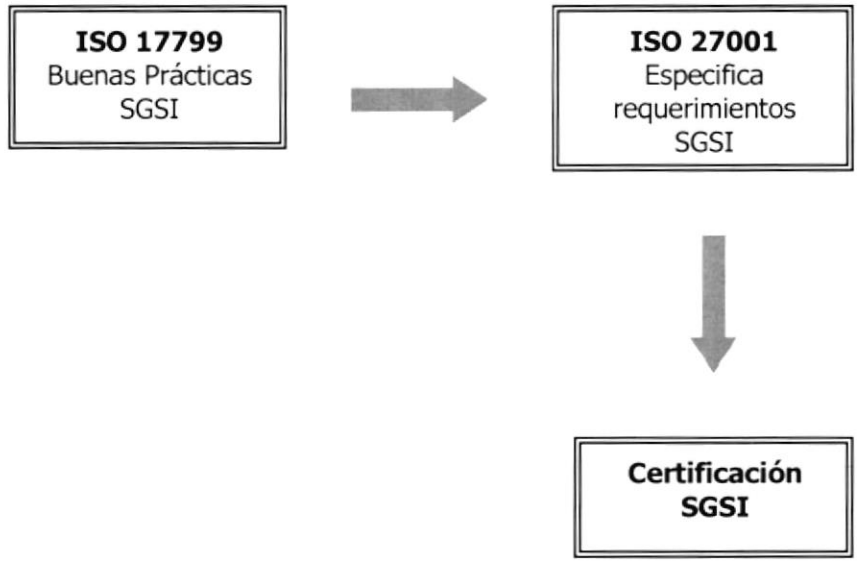


Figura 2.11 Guía para la certificación

La obtención de una certificación del Sistema de Gestión de la Seguridad de la Información, le permite a la organización obtener una ventaja competitiva que le asegura que sus riesgos están administrados. Es importante considerar que con la implementación de un Sistema de Gestión de la Seguridad de la Información los riesgos no son eliminados, sino que se administran y que existe un proceso de mejora continúa.

2.7 El futuro de la Norma ISO 17799

Se ha planteado la creación de una serie de normas orientadas a la seguridad de la información, la serie 27000 dentro de la cual se incluirá a la actual norma ISO 17799:2005

La serie de normas ISO 27000 se plantea de la siguiente forma:

ISO 27000	Vocabulario y definiciones (terminología para todos los demás estándares descritos abajo)
ISO 27001	El estándar principal de requerimientos para un Sistema de Gestión de la Seguridad de la Información. ISO 27001 fue publicada en Octubre del 2005
ISO 27002	La actual ISO 17799 – es el código de prácticas que describen de manera comprensiva, el conjunto de objetivos de control y controles para la seguridad de la información. La version actualizada fue publicada en junio del 2005
ISO 27003	Su contenido será una guía de implementación
ISO 27004	Nuevo estándar de métricas y medidas para administrar la seguridad de la información para ayudar a medir la efectividad de la implementación del sistema de gestión de la seguridad de la información.
ISO 27005	Será un estándar para la administración de riesgos de seguridad de la información (reemplaza al aún no publicado BS 7799 Parte 3)
ISO 27006	Probablemente será un Nuevo estándar: Guía para la recuperación de desastres en los servicios de información y comunicaciones.

Tabla 2.2 Serie de normas ISO 2700

CAPITULO 3

3 Alcance y definición de la tesis

3.1 Objetivos del trabajo

Elaborar el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para la ESCUELA SUPERIOR POLITECNICA DEL LITORAL (ESPOL), así como también presentar las respectivas recomendaciones para su posterior implementación dentro del alcance del presente trabajo.

Dentro del conjunto de beneficios que se obtendrían al contar con un SGSI institucional en ESPOL se pueden mencionar:

- Contar con un proceso definido para: Evaluar, Implementar, Mantener y Administrar la Seguridad de la Información en ESPOL.
- Diferenciarse en el mercado de otras universidades.
- Tener una metodología para poder administrar los riesgos sobre la información que enfrenta ESPOL.

Con el presente trabajo, no se busca preparar a la ESPOL para una eventual certificación en materia de seguridad de la información, sino que proporciona las bases de un SGSI para que una vez implementado, se pueda aprovechar los beneficios que éste ofrece.

3.2 Alcance

El alcance del presente trabajo consiste en el diseño de un SGSI que abarque las principales preocupaciones de la alta gerencia de ESPOL manifestadas durante una entrevista con el equipo de trabajo, (ver ***ANEXO 4.- Entrevistas autoridades ESPOL***) relacionadas con la seguridad de la información basada en la norma ISO 17799:2005 abarcando los dominios:

1.- Política de seguridad de la Información.
2.- Organización de la Seguridad de la Información.
3.- Control de accesos.

Así como también la elaboración de un cronograma propuesto de implementación de los controles identificados para cubrir de manera razonable los riesgos aplicables a ESPOL, en los objetivos de control de los dominios listados anteriormente.

Cabe mencionar que el presente proyecto no incluye la fase de implementación de los controles sugeridos en la parte final para el SGSI.

3.3 Plan de trabajo

En la siguiente tabla se muestra el plan de trabajo empleado en el presente proyecto, donde se describe las etapas, actividades principales y responsabilidades realizadas.

ETAPAS	TAREA	RESPONSABLE		
		MC	DN	EM
ETAPA 1:	ENTENDIMIENTO DE LA ORGANIZACIÓN			
	Levantamiento de información de ESPOL	X	X	X
	Levantamiento de información del CSI		X	
	Entrevista con Directora de CSI	X		X
	Levantamiento de información de la Norma ISO 17799:2005	X	X	X
	Documentación	X	X	X
ETAPA 2:	ENTREVISTAS CON AUTORIDADES			
	Entrevista con Vicerrector General	X	X	X
	Entrevista con Vicerrector Administrativo Financiero	X	X	X
	Entrevista con el Director del CRECE	X		
	Entrevista con Directora del CSI	X	X	X
ETAPA 3:	DEFINICIÓN DEL ALCANCE			
	Análisis de entrevistas con autoridades	X	X	X
	Definir los dominios aplicables para el trabajo	X	X	X
	Documentar la declaración de aplicabilidad			X
	Documentación	X	X	X
ETAPA 4:	EJECUCION DE ANALISIS DE RIESGOS E IDENTIFICACION DE CONTROLES			
	Elaborar el inventario de riesgos	X	X	X
	Identificación y determinación de los riesgos aplicables según los dominios seleccionados		X	
	Evaluación de riesgos	X	X	
	Taller de riesgos con Directora del CSI	X	X	
	Selección de riesgos de mayor severidad	X		
	Selección de controles basados en la norma ISO 17799:2000 para los riesgos severos			X
	Elaborar sugerencias para mitigar los riesgos severos		X	
	Documentación	X	X	X
ETAPA 5:	DISEÑO DE LA PROPUESTA DE IMPLEMENTACION			
	Elaborar propuesta de lineamientos para política de seguridad de la información		X	X
	Elaborar propuesta de implementación de controles determinados		X	X
	Determinar roles requeridos para la implementación del SGSI	X		
	Documentación	X	X	X

MC: Miguel Chang
DN: Dalton Noboa
EM: Ernesto Murrieta

Tabla 3.1 Plan de trabajo

3.4 Metodología de trabajo

A continuación se detalla la descripción de las actividades realizadas dentro del marco metodológico delineado en nuestro plan de trabajo:

ETAPAS	TAREA	DESCRIPCION
ETAPA 1:	**ENTENDIMIENTO DE LA ORGANIZACIÓN**	
	Levantamiento de información de ESPOL	Investigar en el sitio Web de ESPOL información de su estructura orgánica. misión, visión, plan estratégico, infraestructura
	Levantamiento de información del CSI	Determinar los servicios que provee el CSI. Misión, visión, infraestructura, manuales existentes.
	Entrevista con Directora de CSI	Conocer la preocupación de la Directora sobre seguridad de la información en ESPOL
	Levantamiento de información de la Norma ISO 17799:2005	Investigar sobre la versión 2005: dominios, controles, declaración de aplicabilidad. Investigar sobre la norma ISO 27001:2005 Estadísticas relacionadas a la seguridad de la información.
	Documentación	Determinar el índice temático. Escribir sobre conceptos de seguridad de la información. Documentar estadísticas. Documentar información de ESPOL y CSI que se ha encontrado.
ETAPA 2:	**ENTREVISTAS CON AUTORIDADES**	
	Entrevista con Vicerrector General	Efectuar entrevista con Ing. Armando Altamirano, Vicerrector General para determinar: Principales dominios de preocupación Principales objetivos de control de preocupación.
	Entrevista con Vicerrector Administrativo Financiero	Efectuar entrevista con Ing. Jorge Faytong, Vicerrector Administrativo Financiero para determinar: Principales dominios de preocupación Principales objetivos de control de preocupación.
	Entrevista con el Director del CRECE	Efectuar entrevista con Ing. Washington Medina, Director del Centro de Registros y Calificaciones de ESPOL para determinar:

		Principales dominios de preocupación Principales objetivos de control de preocupación.
	Entrevista con Directora del CSI	Efectuar entrevista con MBA. Ruth Álvarez, Directora del Centro de Servicios Informáticos de ESPOL para determinar: Principales dominios de preocupación Principales objetivos de control de preocupación.
ETAPA 3:	**DEFINICIÓN DEL ALCANCE**	
	Análisis de entrevistas con autoridades	Recopilar y realizar el resumen de las entrevistas realizadas.
	Definir los dominios aplicables para el trabajo	Determinar los 3 dominios de mayor preocupación para la alta gerencia en base al resumen de las entrevistas. Determinar los objetivos de control de mayor preocupación para la gerencia, en base a los dominios determinados para el trabajo.
	Documentar la declaración de aplicabilidad	Realizar la documentación de la declaración de aplicabilidad basada en los dominios y objetivos de control seleccionados
	Documentación	Realizar tablas de resumen. Incluir la declaración de aplicabilidad en el documento de la tesis. Determinar anexos para incluir.
ETAPA 4:	**EJECUCION DE ANALISIS DE RIESGOS E IDENTIFICACION DE CONTROLES**	
	Elaborar el inventario de riesgos	Realizar un listado de riesgos generales aplicables a ESPOL
	Identificación y determinación de los riesgos aplicables según los dominios seleccionados	Determinación de los riesgos aplicados a los dominios seleccionados de la lista de inventario de riesgos.
	Evaluación de riesgos	Realizar el análisis de riesgos
	Taller de riesgos con Directora del CSI	Realizar el análisis de riesgos con la Directora del CSI.
	Selección de riesgos de mayor severidad	Comparación de los análisis de riesgos realizados y determinar los riesgos de mayor severidad.

	Selección de controles basados en la norma ISO 17799:2000 para los riesgos severos	Establecer controles para los riesgos severos, basados en la norma ISO 17799:2005
	Elaborar sugerencias para mitigar los riesgos severos	Elaborar una lista de sugerencias aplicables para mitigar los riesgos de mayor severidad.
	Documentación	Incluir en el documento de la tesis el inventario de riesgos, el análisis de riesgos y el listado de controles determinados.
ETAPA 5:	**DISEÑO DE LA PROPUESTA DE IMPLEMENTACION**	
	Elaborar propuesta de lineamientos para política de seguridad de la información	Investigar ejemplos de política de seguridad de la información y elaborar un documento de lineamientos para la definición de una política de seguridad de la información para ESPOL.
	Elaborar propuesta de implementación de controles determinados	Elaborar un cronograma para la implementación de los controles determinados a 2 años. Elaborar el cronograma en períodos de 6 meses y luego detallados por cada mes.
	Determinar roles requeridos para la implementación del SGSI	Investigar sobre roles y responsabilidades del personal asociado a la implementación de un SGSI. Utilizar como referencia material del manual de certificación CISA 2005
	Documentación	Incluir los documentos y tablas elaborados. Revisión del documento con Jorge Olaya Revisión del documento con la Directora del CSI Aplicar formato final a la tesis.

Tabla 3.2 Metodología de trabajo realizada

3.5 Declaración de Aplicabilidad

La declaración de la aplicabilidad es un documento el cual tiene como objetivo proporcionar la justificación para la aplicabilidad o no aplicabilidad de cada control de la norma ISO 17999 al Sistema de Gestión de Seguridad de la Información en cuestión.

En esta declaración deben ser explicados los objetivos, los controles seleccionados y las razones para su selección, como así también las

razones para la exclusión de cualquier medida catalogada en el estándar ISO 17799.

Para mostrar la importancia de la declaración de aplicabilidad, en el ***ANEXO 14.- Ejemplo carta de certificación Banco de Montreal*** presentamos una carta de certificación de un SGSI, donde se hace referencia a la misma.

A continuación se muestra la Declaración de Aplicabilidad del presente trabajo, que resultó del resumen de las entrevistas con las autoridades de ESPOL:

Sección	Objetivo	Control	Aplicación (Si / No)	Documento de referencia o justificación de la exclusión
5	**Política de Seguridad**			
5.1	Política de seguridad de la información	5.1.1 Documentación de la política de seguridad de la información	SI	Preocupaciones de la alta gerencia de ESPOL. Papeles de trabajo con Vicerrector General, Vicerrector Administrativo-Financiero, Director del Centro de Registros, Calificaciones y Estadísticas (CRECE), Directora del Centro de Servicios Informáticos
		5.1.2 Revisión de la política de seguridad de la información	SI	Preocupaciones de la alta gerencia de ESPOL. Papeles de trabajo con Vicerrector General, Vicerrector Administrativo-Financiero, Director del Centro de Registros, Calificaciones y Estadísticas (CRECE), Directora del Centro de Servicios Informáticos
6	**Organización de la Seguridad de la Información**			
6.1	Organización interna	6.1.1 Comité de administración de la seguridad de la información	SI	Preocupación de la alta gerencia por la organización interna. Papel de trabajo con autoridades.
		6.1.2 Coordinación de la seguridad de la información	SI	Preocupación de la alta gerencia por la organización interna. Papel de trabajo con autoridades.
		6.1.3 Asignación de responsabilidades de seguridad de la información	SI	Preocupación de la alta gerencia por la organización interna.

Sección	Objetivo	Control	Aplicación (Si / No)	Documento de referencia o justificación de la exclusión
				Papel de trabajo con autoridades.
		6.1.4 Proceso de autorización para instalaciones de procesamiento de información	SI	Preocupación de la alta gerencia por la organización interna. Papel de trabajo con autoridades.
		6.1.5 Acuerdos de confidencialidad	SI	Preocupación de la alta gerencia por la organización interna. Papel de trabajo con autoridades.
		6.1.6 Contacto y autoridades	SI	Preocupación de la alta gerencia por la organización interna. Papel de trabajo con autoridades.
		6.1.7 Contactos con grupos especiales de interés	SI	Preocupación de la alta gerencia por la organización interna. Papel de trabajo con autoridades.
		6.1.8 Revisión independiente de la seguridad de la información	SI	Preocupación de la alta gerencia por la organización interna.
6.2	Partes externas	6.2.1 Identificación de los riesgos relacionados a partes externas	NO	No se define en el alcance
		6.2.2 Direccionamiento de la seguridad cuando se trate con partes externas	NO	No se define en el alcance
		6.2.3 Direccionamiento de seguridad en acuerdos con terceras partes	NO	No se define en el alcance
7	**Administración de activos**			
7.1	Responsabilidad de activos	7.1.1 Inventario de activos	NO	No se define en el alcance
		7.1.2 Propietario de activos	NO	No se define en el alcance
		7.1.3 Uso aceptable de activos	NO	No se define en el alcance

Sección	Objetivo	Control	Aplicación (Si / No)	Documento de referencia o justificación de la exclusión
7.2	Clasificación de la información	7.2.1 Pautas de clasificación	NO	No se define en el alcance
		7.2.2 Rotulado y manejo de la información	NO	No se define en el alcance
8	**Seguridad del Recurso Humano**			
8.1	Etapa previa al empleo	8.1.1 Roles y responsabilidades	NO	No se define en el alcance
		8.1.2 Investigación	NO	No se define en el alcance
		8.1.3 Términos y condiciones de empleo	NO	No se define en el alcance
8.2	Durante el empleo	8.2.1 Administración de responsabilidad	NO	No se define en el alcance
		8.2.2 Conocimiento, educación y entrenamiento de la seguridad de la información.	NO	No se define en el alcance
		8.2.3 Proceso disciplinario	NO	No se define en el alcance
8.3	Terminación o cambio de empleo	8.3.1 Terminación de responsabilidades	NO	No se define en el alcance
		8.3.2 Retorno de activos	NO	No se define en el alcance
		8.3.3 Remoción de derechos de acceso	NO	No se define en el alcance
9	**Seguridad Física y Ambiental**			
9.1	Áreas seguras	9.1.1 Seguridad del perímetro físico	NO	No se define en el alcance
		9.1.2 Controles de entrada físicos	NO	No se define en el alcance
		9.1.3 Seguridad en oficinas, cuartos y ambientes	NO	No se define en el alcance
		9.1.4 Protección contra amenazas externas	NO	No se define en el alcance
		9.1.5 Trabajo en áreas seguras	NO	No se define en el alcance
		9.1.6 Áreas de carga, entrega y acceso público	NO	No se define en el alcance
9.2	Seguridad del equipo	9.2.1 Ubicación y protección del equipo	NO	No se define en el alcance
		9.2.2 Utilidades de soporte	NO	No se define en el alcance
		9.2.3 Seguridad del cableado	NO	No se define en el alcance
		9.2.4 Mantenimiento de equipos	NO	No se define en el alcance
		9.2.5 Seguridad del equipo off-premises	NO	No se define en el alcance
		9.2.6 Disposición segura o re-uso de equipo	NO	No se define en el alcance
		9.2.7 Retiro de propiedad	NO	No se define en el alcance
10	**Administración de las Comunicaciones y Operación**			
10.1	Procedimientos y responsabilidades	10.1.1 Procedimientos operativos documentados	NO	No se define en el alcance

Sección	Objetivo	Control	Aplicación (Si / No)	Documento de referencia o justificación de la exclusión
	operativas	10.1.2 Administración de cambios	NO	No se define en el alcance
		10.1.3 Segregación de funciones	NO	No se define en el alcance
		10.1.4 Separación de las facilidades de desarrollo y operación	NO	No se define en el alcance
10.2	Administración de la entrega de servicio por terceras partes	10.2.1 Entrega del servicio	NO	No se define en el alcance
		10.2.2 Monitoreo y revisión de servicios de terceras partes	NO	No se define en el alcance
		10.2.3 Manejo de cambios a servicios de terceras partes	NO	No se define en el alcance
10.3	Planeación de sistemas y aceptación	10.3.1 Capacidad de administración	NO	No se define en el alcance
		10.3.2 Aceptación de sistemas	NO	No se define en el alcance
10.4	Protección contra código malicioso	10.4.1 Controles contra código malicioso	NO	No se define en el alcance
		10.4.2 Controles contra código móvil	NO	No se define en el alcance
10.5	Respaldos	10.5.1 Información de respaldos	NO	No se define en el alcance
10.6	Administración de la seguridad de la red	10.6.1 Controles de la red	NO	No se define en el alcance
		10.6.2 Seguridad en los servicios de la red	NO	No se define en el alcance
10.7	Manejo de medios	10.7.1 Manejo de medios removibles	NO	No se define en el alcance
		10.7.2 Disposición de medios	NO	No se define en el alcance
		10.7.3 Procedimientos de manejo de información	NO	No se define en el alcance
		10.7.4 Seguridad de la documentación del sistema	NO	No se define en el alcance
10.8	Intercambio de información / Servicios de comercio electrónico	10.8.1 Políticas y procedimientos de intercambio de información	NO	No se define en el alcance
		10.8.2 Acuerdos de intercambio	NO	No se define en el alcance
		10.8.3 Medios físicos en tránsito	NO	No se define en el alcance
		10.8.4 Mensajería electrónica	NO	No se define en el alcance
		10.8.5 Sistemas de información del negocio	NO	No se define en el alcance
10.9	Servicios de comercio electrónico	10.9.1 Comercio electrónico	NO	No se define en el alcance
		10.9.2 Transacciones en línea	NO	No se define en el alcance
		10.9.3 Información disponible públicamente	NO	No se define en el alcance

Sección	Objetivo	Control	Aplicación (Si / No)	Documento de referencia o justificación de la exclusión
10.10	Monitoreo	10.10.1 Log de auditoria	NO	No se define en el alcance
		10.10.2 Monitoreo del uso del sistema	NO	No se define en el alcance
		10.10.3 Protección de la información del log	NO	No se define en el alcance
		10.10.4 Administración y operación de logs	NO	No se define en el alcance
		10.10.5 Fallas de log	NO	No se define en el alcance
		10.10.6 Sincronización del reloj	NO	No se define en el alcance
11	**Control de accesos**			
11.1	Requerimientos del negocio para control de acceso	11.1.1 Política de control de acceso	SI	Preocupación de la alta gerencia por los accesos. Papel de trabajo con autoridades.
11.2	Administración de accesos de usuarios	11.2.1 Registro de usuario	NO	No se define en el alcance
		11.2.2 Medición de privilegios	NO	No se define en el alcance
		11.2.3 Administración del password de usuarios	NO	No se define en el alcance
		11.2.4 Revisión de privilegios de accesos de usuarios	NO	No se define en el alcance
11.3	Responsabilidades del usuario	11.3.1 Uso de password	SI	Preocupación de la alta gerencia por la responsabilidad de los usuarios. Papel de trabajo con autoridades.
		11.3.2 Equipos desatendidos de usuarios	SI	Preocupación de la alta gerencia por la responsabilidad de los usuarios. Papel de trabajo con autoridades.
		11.3.3 Políticas de pantalla de PC y escritorio limpio	SI	Preocupación de la alta gerencia por la responsabilidad de los usuarios. Papel de trabajo con autoridades.
11.4	Control de acceso a la red	11.4.1 Políticas en el uso de los servicios de la red	NO	No se define en el alcance
		11.4.2 Autenticación de usuarios para conexiones externas	NO	No se define en el alcance

Sección	Objetivo	Control	Aplicación (Si / No)	Documento de referencia o justificación de la exclusión
		11.4.3 Identificación de equipos en redes	NO	No se define en el alcance
		11.4.4 Diagnóstico remoto y configuración de protección de puertos	NO	No se define en el alcance
		11.4.5 Segregación en redes	NO	No se define en el alcance
		11.4.6 Control en la conexión de la red	NO	No se define en el alcance
		11.4.7 Control en el ruteo de la red	NO	No se define en el alcance
11.5	Control de acceso al sistema operativo	11.5.1 Procedimientos seguros de Log-on	NO	No se define en el alcance
		11.5.2 Identificación y autenticación de usuario	NO	No se define en el alcance
		11.5.3 Sistema de administración de password	NO	No se define en el alcance
		11.5.4 Uso de utilidades del sistema	NO	No se define en el alcance
		11.5.5 Time-out de sesiones	NO	No se define en el alcance
		11.5.6 Límite en el tiempo de conexión	NO	No se define en el alcance
11.6	Control de acceso a aplicaciones	11.6.1 Restricción de accesos a la información	SI	Preocupación de la alta gerencia en las aplicaciones. Papel de trabajo con autoridades.
		11.6.2 Aislamiento sensible del sistema	SI	Preocupación de la alta gerencia en las aplicaciones. Papel de trabajo con autoridades.
11.7	Computación móvil y teletrabajo	11.7.1 Computación y comunicación móvil	NO	No se define en el alcance
		11.7.2 Teleworking	NO	No se define en el alcance
12	**Adquisición, desarrollo y mantenimiento de sistemas de información**			
12.1	Requerimientos de seguridad en sistemas de información	12.1.1 Análisis y especificaciones de requerimientos de seguridad	NO	No se define en el alcance
12.2	Correcto procesamiento en las aplicaciones	12.2.1 Validación de ingreso de datos	NO	No se define en el alcance
		12.2.2 Control de procesamiento interno	NO	No se define en el alcance
		12.2.3 Integridad de mensajes	NO	No se define en el alcance
		12.2.4 Validación de la salida de datos	NO	No se define en el alcance
12.3	Controles criptográficos	12.3.1 Política en el uso de controles criptográficos	NO	No se define en el alcance
		12.3.2 Administración de claves	NO	No se define en el alcance

Sección	Objetivo	Control	Aplicación (Si / No)	Documento de referencia o justificación de la exclusión
12.4	Seguridad de los archivos del sistema	12.4.1 Control de operaciones de software	NO	No se define en el alcance
		12.4.2 Protección de datos de prueba del sistema	NO	No se define en el alcance
		12.4.3 Control de accesos a la librería de fuentes de los programas	NO	No se define en el alcance
12.5	Seguridad de los procesos de desarrollo y soporte	12.5.1 Procedimientos de control de cambios	NO	No se define en el alcance
		12.5.2 Revisiones técnicas de aplicaciones después de operaciones de cambios al sistema	NO	No se define en el alcance
		12.5.3 Restricciones de cambios en los paquetes de software	NO	No se define en el alcance
		12.5.4 Salida de la información	NO	No se define en el alcance
		12.5.5 Desarrollo de software en outsourcing	NO	No se define en el alcance
12.6	Administración de vulnerabilidades técnicas	12.6.1 Control de vulnerabilidades técnicas	NO	No se define en el alcance
13	**Administración de incidentes de seguridad de la información**			
13.1	Reportes de eventos y debilidades de la seguridad de la información	13.1.1 Reporte de eventos de seguridad de la información	NO	No se define en el alcance
		13.1.2 Divulgación de debilidades de la seguridad	NO	No se define en el alcance
13.2	Gestión de incidentes y mejoras de la seguridad de la información	13.2.1 Responsabilidades y procedimientos	NO	No se define en el alcance
		13.2.2 Aprender de los incidentes de seguridad de la información	NO	No se define en el alcance
		13.2.3 Colección de evidencia	NO	No se define en el alcance
14	**Administración de la continuidad del negocio**			
14.1	Aspectos de la administración de la continuidad de los negocios	14.1.1 Incluir la seguridad de la información en los procesos de administración de la continuidad del negocio	NO	No se define en el alcance
		14.1.2 Continuidad del negocio y evaluación de riesgos	NO	No se define en el alcance
		14.1.3 Desarrollo e implementación de planes de continuidad incluyendo la seguridad de la información	NO	No se define en el alcance
		14.1.4 Marco del planeamiento de la continuidad	NO	No se define en el alcance

Sección	Objetivo	Control	Aplicación (Si / No)	Documento de referencia o justificación de la exclusión
		del negocio		
		14.1.5 Pruebas, mantenimiento y re-valoración de los planes de continuidad	NO	No se define en el alcance
15	**Cumplimiento**			
15.1	Cumplimiento de requisitos legales	15.1.1 Identificación de leyes aplicables	NO	No se define en el alcance
		15.1.2 Derechos de propiedad intelectual	NO	No se define en el alcance
		15.1.3 Protección de registros organizacionales	NO	No se define en el alcance
		15.1.4 Protección de datos y privacidad de la información personal	NO	No se define en el alcance
		15.1.5 Prevención del uso erróneo de instalaciones de tratamiento de la información	NO	No se define en el alcance
		15.1.6 Regulación de los controles criptográficos	NO	No se define en el alcance
15.2	Cumplimiento con la política de seguridad, estándares y cumplimientos técnicos	15.2.1 Cumplimiento con la política de seguridad	NO	No se define en el alcance
		15.2.2 Revisión de cumplimiento técnico	NO	No se define en el alcance
15.3	Consideraciones de auditoria de sistemas de información	15.3.1 Auditoria de controles de sistemas de información	NO	No se define en el alcance
		15.3.2 Auditoria de herramientas de protección de sistemas de información	NO	No se define en el alcance

Tabla 3.3 Declaración de aplicabilidad

Nota Final:

El alcance definido en la presente declaración de aplicabilidad se ha definido en base a los siguientes parámetros:

- La prioridad expresada por las autoridades que se entrevistaron
- El tiempo disponible para la realización del presente trabajo

CAPITULO 4

4 Análisis de riesgos

4.1 Marco Teórico

4.1.1 Introducción

Cuando se habla de seguridad de la información hay que establecer los requerimientos de seguridad; es esencial que una organización logre identificar sus requerimientos de seguridad, para esto existen tres recursos principales para lograrlos:

El primer recurso consiste en evaluar los riesgos que enfrenta la organización. Mediante el análisis de riesgos se identifican las amenazas a los activos, se evalúan las vulnerabilidades y probabilidad de ocurrencia, y se estima el impacto potencial.

El segundo recurso está constituido por los requisitos legales, normativos, reglamentarios y contractuales que deben cumplir la organización, sus socios comerciales, los contratistas y los prestadores de servicios.

El tercer recurso es el conjunto específico de principios, objetivos y requisitos para el procesamiento de la información, que ha desarrollado la organización para respaldar sus operaciones.

Los requerimientos de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad. Las erogaciones derivadas de la satisfacción de las necesidades de control deben ser equilibradas con respecto al impacto potencial de las fallas de seguridad en los negocios. Las técnicas de evaluación de riesgos pueden aplicarse a toda la organización, o sólo a partes de la misma, así como a los sistemas de información individuales, componentes de sistemas o servicios específicos cuando esto resulte factible, viable y provechoso.

4.1.2 Definición de análisis de riesgo

El análisis de riesgos es realizado para detectar los riesgos a los cuales están sometidos los activos de una organización, es decir, para saber cuál es la probabilidad de que las amenazas se concreten.

Las amenazas se pueden convertir en realidad a través de fallas de seguridad, que conocemos como vulnerabilidades y que deben ser

eliminadas al máximo para que el ambiente que se desea proteger esté libre de riesgos de incidentes de seguridad.

Por lo tanto, la relación entre amenaza-incidente-impacto, es la condición principal a tomar en cuenta en el momento de priorizar acciones de seguridad para la corrección de los activos que se desean proteger

4.1.3 Objetivos del Análisis de riesgo

El análisis de riesgo tiene como objetivo:
Estudiar los riesgos que soporto una determinada área relativa a las tecnologías de información y el entorno asociable con esta. Estimando la probabilidad de ocurrencia y el nivel de impacto que puede ocasionar si el riesgo se llega a materializar.
Recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados.

4.1.4 Clasificación de Riesgos de negocios relacionados con la informática

Los principales riesgos informáticos de los negocios son los siguientes:

- **Riesgos de Integridad:** Este tipo abarca todos los riesgos asociados con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas en una organización. Estos riesgos se manifiestan en los siguientes componentes de un sistema:

    - Interfase del usuario: Los riesgos en esta área generalmente se relacionan con las restricciones, sobre las individualidades de una organización y su autorización de ejecutar funciones negocio/sistema; teniendo en cuenta sus necesidades de trabajo y una razonable segregación de obligaciones.

    - Procesamiento: Los riesgos en esta área generalmente se relacionan con el adecuado balance de los controles detectivos y preventivos que aseguran que el procesamiento de la información ha sido completado.

    - Procesamiento de errores: Los riesgos en esta área generalmente se relacionan con los métodos que aseguren que cualquier entrada/proceso de información de errores sean capturados adecuadamente, corregidos y reprocesados con exactitud completamente.

- Interfase: Los riesgos en esta área generalmente se relacionan con controles preventivos y detectivos que aseguran que la información ha sido procesada y transmitida adecuadamente por las aplicaciones.

- Administración de cambios: Los riesgos en esta área pueden ser generalmente considerados como parte de la infraestructura de riesgos y el impacto de los cambios en las aplicaciones.

- Información: Los riesgos en esta área pueden ser generalmente considerados como parte de la infraestructura de las aplicaciones. Estos riesgos están asociados con la administración inadecuada de controles, incluyendo la integridad de la seguridad de la información procesada y la administración efectiva de los sistemas de bases de datos y de estructuras de datos. La integridad puede perderse por: Errores de programación (buena información es procesada por programas mal construidos), procesamiento de errores (transacciones incorrectamente procesadas) ó administración y procesamiento de errores (Administración pobre del mantenimiento de sistemas).

- **Riesgos de relación:** Los riesgos de relación se refieren al uso oportuno de la información creada por una aplicación. Estos riesgos se relacionan directamente a la información de toma de decisiones.

- **Riesgos de acceso:** Estos riesgos se enfocan al inapropiado acceso a sistemas, datos e información. Estos riesgos abarcan: Los riesgos de segregación inapropiada de trabajo, los riesgos asociados con la integridad de la información de sistemas de bases de datos y los riesgos asociados a la confidencialidad de la información.

    - Procesos de negocio: Las decisiones organizacionales deben separar trabajo incompatible de la organización y proveer el nivel correcto de ejecución de funciones.

    - Aplicación: La aplicación interna de mecanismos de seguridad que provee a los usuarios las funciones necesarias para ejecutar su trabajo.

    - Administración de la información: El mecanismo provee a los usuarios acceso a la información específica del entorno.

    - Entorno de procesamiento: Estos riesgos en esta área están manejados por el acceso inapropiado al entorno de programas e información.

- Redes: En esta área se refiere al acceso inapropiado al entorno de red y su procesamiento.

- Nivel físico: Protección física de dispositivos y un apropiado acceso a ellos.

- **Riesgos de utilidad:** Estos riesgos se enfocan en tres diferentes niveles de riesgo:

  - Los riesgos pueden ser enfrentados por el direccionamiento de sistemas antes de que los problemas ocurran.

  - Técnicas de recuperación/restauración usadas para minimizar la ruptura de los sistemas.

  - Backups y planes de contingencia controlan desastres en el procesamiento de la información.

- **Riesgos en la infraestructura:** Estos riesgos se refieren a que en las organizaciones no existe una estructura información tecnológica efectiva (hardware, software, redes, personas y procesos) para soportar adecuadamente las necesidades futuras y presentes de los negocios con un costo eficiente.

  - Planeación organizacional: Los proceso en esta área aseguran la definición del impacto, definición y verificación de la tecnología informática en el negocio. Además, verifica si existe una adecuada organización (gente y procesos) asegura que los esfuerzos de la tecnología informática será exitosa.

  - Definición de las aplicaciones: Los procesos en esta área aseguran que las aplicaciones satisfagan las necesidades del usuario y soporten el contexto de los procesos de negocio.

  - Administración de seguridad: Los procesos en esta área aseguran que la organización está adecuadamente direccionada a establecer, mantener y monitorizar un sistema interno de seguridad, que tenga políticas de administración con respecto a la integridad y confidencialidad de la información de la organización, y a la reducción de fraudes a niveles aceptables.

  - Operaciones de red y computacionales: Los procesos en esta área aseguran que los sistemas de información y entornos de red están operados en un esquema seguro y protegido, y que las responsabilidades de procesamiento de información son ejecutados por personal operativo definido, medido y monitoreado.

- Administración de sistemas de bases de datos: Los procesos en esta área están diseñados para asegurar que las bases de datos usadas para soportar aplicaciones críticas y reportes tengan consistencia de definición, correspondan con los requerimientos y reduzcan el potencial de redundancia.

- Información / Negocio: Los proceso en esta área están diseñados para asegurar que existe un plan adecuado para asegurar que la tecnología informática estará disponible a los usuarios cuando ellos la necesitan.

- **Riesgos de seguridad general:**

  - Riesgos de choque de eléctrico: Niveles altos de voltaje.
  - Riesgos de incendio: Inflamabilidad de materiales.
  - Riesgos de niveles inadecuados de energía eléctrica.
  - Riesgos de radiaciones: Ondas de ruido, de láser y ultrasónicas.
  - Riesgos mecánicos: Inestabilidad de las piezas eléctricas.

4.1.5 Estructura del análisis de riesgo.

Para poder llevar acabo un análisis de riegos se tiene que cubrir los siguientes puntos:

Objetivos del Análisis de riesgo.- El establecimiento de los objetivos del análisis es el primer paso que se debe realizar, por lo general los objetivos más comunes son:

- Identificar los riesgos aplicables para la organización.
- Identificar los riegos de mayor severidad, los que causen un mayor impacto sobre los activos de la organización.
- Establecimiento de controles que permitan mitigar los riesgos más severos.

Identificación de los riesgos.- Antes de enfrentar los riesgos, estos deben ser identificarlos. Esta tarea es perenne, pues nuevas amenazas están surgiendo constantemente. La identificación de riesgos es continua y depende de la red de comunicación dentro de la organización, generando un flujo constante de información acerca de las actividades de la organización.

Evaluación de los riesgos.- Es la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto sobre los activos de la organización. El resultado de la evaluación es la determinación de los riesgos más severos que se presentan en la organización.

Controles.- Una vez evaluados los riesgos e identificados cuales son los de mayor severidad se deben establecer ciertos controles que ayuden a solucionar o mitigar los riesgos.

4.2 Análisis de Riesgo para ESPOL

4.2.1 Introducción

De acuerdo a la declaración de la aplicabilidad de ESPOL, establecida en base a la delimitación del alcance definido en las entrevistas con las Principales Autoridades de ESPOL: Ing. Armando Altamirano, Vicerrector General; Ing. Jorge Fayton, Vicerrector Financiero; Ing. Washington Medina, Director del Centro de Registros Calificaciones y Estadísticas de ESPOL;(ver ***ANEXO 4.- Entrevistas autoridades ESPOL***), sobre los dominios de la norma ISO 17799 sobre los cuales se trabajara son: Política de Seguridad, Organización de la seguridad de la información y Control de accesos, por ende el análisis de riesgo se concentrara en los mismos, identificando los riegos aplicables dentro de cada uno de los dominios, realizando una evaluación de riesgo para determinar cuales son las amenazas sobre las cuales hay que establecer controles.

4.2.2 Objetivos del Análisis de Riesgos

Es objetivo que pretende alcanzar este análisis es conocer cuales son los riegos de mayor severidad dentro de los dominios de estudio para la información que administra el CSI.

4.2.3 Identificación de riesgos.

En este punto se desarrollo un inventario de riesgos (ver ***ANEXO 12.- Inventario de riesgos***) producto de una investigación acerca de los mismos en Internet, el entorno del Centro de Servicios Informáticos, entrevista con el personal de CSI y visitas realizadas centro de computo.

El inventario consta de 133 riesgos, de los cuales mediante la clasificación y encasillamiento de los mismos dentro de los dominios establecidos en la declaración de aplicabilidad, se determinó que 65 son aplicables a ESPOL.

Dominios	Cantidad
Política de Seguridad	11
Organización de la seguridad de la información	17
Control de accesos	37
Otros	78
Total	133

Tabla 4.1 Resumen de la identificación de riesgos

4.2.4 Evaluación de Riesgos

En la evaluación de riesgos se manejan tres aspectos fundamentales como son: La probabilidad de ocurrencia, el nivel de impacto y la severidad. Para cada uno de estos se detalla a continuación el esquema con el que se trabajo.

4.2.5 Probabilidad de Ocurrencia

No existe un estándar definido para la escala del nivel de ocurrencia. Para la clasificación de los riesgos más probables se utilizo la siguiente estructura:

Calificación	Nivel de Ocurrencia
Muy Alta	8
Alta (Media +)	6
Baja (Media -)	4
Muy Baja	2

Tabla 4.2 Calificación de riesgo de acuerdo al Nivel de ocurrencia

De acuerdo a la clasificación anterior se considera a los riesgos más probables a los que obtengan un nivel de ocurrencia de 8 o 6, y a los menos probables los que obtengan un nivel de ocurrencia 4 o 2.

4.2.6 Nivel de Impacto

No existe un estándar definido para la escala del nivel de impacto. Para la clasificación de los riesgos de mayor nivel de impacto se utilizo la siguiente estructura:

Calificación	Nivel de Impacto
Muy Alta	10
Alta (Media +)	8
Media	6
Baja (Media -)	4
Muy Baja	2

Tabla 4.3 Calificación de riesgo de acuerdo a su Nivel de impacto

De acuerdo a la clasificación anterior se considera a los riesgos que causan un mayor nivel de impacto sobre los activos a los que obtengan un nivel de 10 o 8, el nivel de impacto 6 se considera como un impacto medio sobre el activo, y los que obtengan un nivel de impacto de 4 o 2 son considerados de menor impacto.

4.2.7 Severidad

Para la obtención de la severidad de los riesgos se utilizo la siguiente igualdad:

Severidad = Nivel de Ocurrencia x Nivel de Impacto

De acuerdo a la igualdad anterior y a los niveles de ocurrencia e impacto, se pueden presentar 20 posibles combinaciones siendo la de menor valor de severidad 4 y la de mayor valor de severidad 80.
Para la clasificación de la severidad para los riesgos se aplico el siguiente criterio, la división de acuerdo a tres niveles de severidad:
Riesgos de severidad baja.- Acumula el 33% de los valores de severidad. Es decir los que obtenga un valor de severidad comprendido entre 4 y 20.
Riesgos de severidad media.- Entre el 33% y 66% de los valores de severidad. Es decir los que obtenga un valor de severidad entre 24 y 36.
Riesgos de severidad alta.- Mayor al 66% de los valores de severidad. Es decir los que obtenga un valor de severidad mayor 48.

Nivel Severidad	Etiqueta	Mínimo	Máximo
Severidad baja	B	4	20
Severidad Media	M	24	36
Severidad Alta	A	48	80

Tabla 4.4 Clasificación de Riesgos de acuerdo a al nivel de severidad

De acuerdo con la clasificaron anterior se establecerán controles para los riesgos de mayor severidad o severidad alta.

4.2.8 Ejecución de la evaluación de riesgo

A continuación en la Tabla 4.5, se detalla la estimación de los niveles de ocurrencia e impacto de los riesgos aplicables a ESPOL realizados en un taller de manera conjunta entre Miguel Chang, Dalton Noboa, Ernesto Murrieta y La MBA. Ruth Álvarez Directora del CSI-ESPOL (ver ***ANEXO 13.- Asignación de probabilidad vs. impacto a riesgos aplicables***).

Las celdas resaltadas indican aquellos riesgos con calificaciones mayores que fueron considerados como los de mayor severidad para la ejecución del presente trabajo y se resumen en la Tabla 4.6.

Dominio	Objetivo de Control	Riesgo	Nivel de Ocurrencia	Nivel de Impacto	Severidad
Política de Seguridad	**Políticas de Seguridad de la Información**	No existe un organigrama de la estructura organizacional del personal de Tecnología Información o que no se encuentre actualizado.	2	6	12
		No exista una política de seguridad de la información formalmente establecida.	6	6	36
		Exista una política de seguridad de la información que no ha sido conocida por todo el personal.	6	8	**48**
		No contar con políticas y procedimientos respaldos y de recuperación de información.	4	10	40
		Exista una política de seguridad de la información no alineada con los objetivos de la organización.	2	8	16
		No existe control sobre los documentos del centro de cómputo.	4	6	24
		Existe una política de seguridad desactualizada.	6	8	**48**
	Documentación de la política de seguridad de la información	No existe un organigrama de la estructura organizacional del personal de Tecnología Información.	2	6	12
		No exista una política de seguridad de la información formalmente establecida.	6	6	36
		No contar con políticas y procedimientos respaldos y de recuperación de información.	6	10	**60**
		Exista una política de seguridad de la información no alineada con los objetivos de la organización.	4	8	32

Organización de la Seguridad	**Infraestructura de seguridad de la información**	No contar con un manual de funciones del personal, o no tenerlo actualizado.	4	6	24
		No exista una política de seguridad de la información formalmente establecida.	6	6	36
		No exista la adecuada segregación de funciones.	2	6	12
		No exista un personal encargado de la revisión y mantenimiento de la política de seguridad de la información.	6	6	36
		No existen procedimientos / controles para modificación del software.	6	10	**60**
		No existen procedimientos de respaldo.	6	8	**48**
		No existen procedimientos de recuperación.	6	8	**48**
		No existe control de los cartuchos de respaldos.	2	4	8
		No se realiza una revisión de los respaldos (backups).	4	10	40
		Daño o pérdidas de respaldos de información por almacenamiento indebido.	4	10	40
		No tener documentación adecuada que respalde las operaciones realizadas.	6	10	**60**
		Aplicaciones de procedimientos erróneos al momento de generar los respaldos o de recuperar la información.	4	8	32
		No se encuentre separada las áreas de desarrollo con la de producción.	6	10	**60**
		No exista un responsable de la administración de la Base de Datos.	2	10	20
		Imposibilidad para evaluar la validez de la transacción debido a posibles manipulaciones de la base de datos, por ausencia de pistas de auditorias.	4	10	40

		No se encuentre separada la bases de datos en producción de la bases de datos pruebas	2	8	16
		Los cambios sobre la bases de datos no pasen por una previa aprobación.	4	6	24

Control de Accesos	**Responsabilidades del Usuario**	Divulgación de password, o que los password se encuentre a la vista de todos.	4	10	40
		Divulgación de dirección de correo electrónico o de información confidencial por Internet.	no contesta		
		Uso de software ilegal, no autorizado, pirata o compartido.	8	8	**64**
		Ingeniería Social.	8	10	**80**
		Spam.	6	8	**48**
	Requerimientos del negocio para control de acceso	No existen políticas para la creación de passwords.	2	6	12
		No existen procedimientos de actualización periódica de passwords.	4	8	32
		No existen perfiles de usuarios definidos.	4	8	32
		No poseen sistemas de cifrado de passwords.	4	8	32
		El formato de password (número de caracteres alfanuméricos) no sea el adecuado.	2	6	12
		No se verifica el acceso no autorizado a computadoras del personal.	2	10	20
		No se tiene instalado software antivirus en las computadoras	4	8	32
		No se realiza una actualización periódica del software antivirus instalado.	6	8	**48**
		No se realiza una exploración periódica de virus en los computadores.	4	8	32

		No existen procedimientos para soporte a usuarios.	4	6	24
		Solo exista una persona encargada de la administración de las claves.	4	8	32
		No detectar oportunamente accesos indebidos o posibles violaciones de seguridad en la base de datos.	4	10	40
		Manipulación de los datos de la Base Datos por parte de usuarios no autorizados (modificaciones o eliminaciones).	2	10	20
		Imposibilidad de identificar las autorizaciones y motivos de los cambios realizados por Ausencia de pistas de auditorias.	6	10	**60**
		Extracción de información confidencial.	2	8	16
		Personal no autorizado accese al centro de cómputo.	6	8	**48**
		No exista chapas de seguridad eléctrica u otro mecanismo de control de ingreso en el área de servidores.	6	8	**48**
		No se registren los ingresos del personal al centro de cómputo en una bitácora.	8	8	**64**
		No se cambie periódicamente códigos de acceso digitales si existiera esta tecnología en el centro de cómputo.	8	8	**64**
		No exista un responsable de la seguridad del acceso físico al centro cómputo.	6	8	**48**
		Que en la política de seguridad no se considere el acceso físico al centro cómputo.	6	8	**48**
		Exista solo una persona encargada de las llaves del centro de cómputo.	6	10	**60**

		El área de servidores no sea la adecuada en el centro de cómputo.	6	8	**48**
		No existan las respectivas señales de advertencia de acceso o emergencias en el centro de cómputo.	6	8	**48**
		Las puertas y ventanas del centro de cómputo queden abiertas al final de un día de laboral.	4	8	32
		Personal de programación tenga acceso al área de bibliotecas de programas de sistemas.	4	6	24
	Control de acceso a la aplicación	Posible incursión de hackers en el sistema	4	8	32
		No se encuentre activado el área de log en donde se registre el acceso a los sistemas	6	8	**48**
		No exista el personal encargado de la revisión del área de log de acceso al sistema	6	8	**48**
		Incursión de terceros malintencionados pueden tener acceso a aplicaciones críticas o a datos valiosos por medio del uso de las debilidades en el software de comunicaciones y protocolos de red. (incluido red inalámbrica)	4	10	40
		No exista un mecanismo adecuado que valide el acceso a los sistema desde la parte externa(Confirmación de llamada, verificación de la redundancia)	6	8	**48**
		Las aplicaciones o programas solo interactúen con lo necesario de la base de datos más no con el total de la misma.	6	8	**48**

Tabla 4.5.- Análisis de riesgo

Dominio	Objetivo de Control	Riesgo	Nivel de Ocurrencia	Nivel de Impacto	Severidad
Política de Seguridad	**Políticas de Seguridad de la Información**	Exista una política de seguridad de la información que no ha sido conocida por todo el personal.	6	8	**48**
		Existe una política de seguridad desactualizada.	6	8	**48**
	Documentación de la política de seguridad de la información	No contar con políticas y procedimientos respaldos y de recuperación de información.	6	10	**60**
Organización de la Seguridad	**Organización Interna**	No existen procedimientos / controles para modificación del software.	6	10	**60**
		No existen procedimientos de respaldo.	6	8	**48**
		No existen procedimientos de recuperación.	6	8	**48**
		No tener documentación adecuada que respalde las operaciones realizadas.	6	10	**60**
		No se encuentre separada las áreas de desarrollo con la de producción.	6	10	**60**
Control de Accesos	**Responsabilidades del Usuario**	Uso de software ilegal, no autorizado, pirata o compartido.	8	8	**64**
		Ingeniería Social.	8	10	**80**
		Spam.	6	8	**48**

	Requerimientos del negocio para control de acceso	No se realiza una actualización periódica del software antivirus instalado.	6	8	**48**
		Imposibilidad de identificar las autorizaciones y motivos de los cambios realizados por Ausencia de pistas de auditorias.	6	10	**60**
		No exista chapas de seguridad eléctrica u otro mecanismo de control de ingreso en el área de servidores.	6	8	**48**
		No se registren los ingresos del personal al centro de cómputo en una bitácora.	8	8	**64**
		No se cambie periódicamente códigos de acceso digitales si existiera esta tecnología en el centro de cómputo.	8	8	**64**
		No exista un responsable de la seguridad del acceso físico al centro cómputo.	6	8	**48**
		Que en la política de seguridad no se considere el acceso físico al centro cómputo.	6	8	**48**
		Exista solo una persona encargada de las llaves del centro de cómputo.	6	10	**60**
		El área de servidores no sea la adecuada en el centro de cómputo.	6	8	**48**
		No existan las respectivas señales de advertencia de acceso o emergencias en el centro de cómputo.	6	8	**48**
		Personal no autorizado accese al centro de cómputo.	8	6	**48**
	Control de acceso a la aplicación	No se encuentre activado el área de log en donde se registre el acceso a los sistemas	6	8	**48**
		No exista el personal encargado de la revisión del área de log de acceso al sistema	6	8	**48**

		No exista un mecanismo adecuado que valide el acceso a los sistema desde la parte externa(Confirmación de llamada, verificación de la redundancia)	6	8	**48**
		Las aplicaciones o programas solo interactúen con lo necesario de la base de datos más no con el total de la misma.	6	8	**48**

Tabla 4.6.- Riesgos más severos resultado del análisis de riesgos

CAPITULO 5

5 Controles

5.1 Marco teórico

El control establece la parte medible o cuantificable al trabajo, no existe control que por su naturaleza no pueda ser cuantificado con lo cual se establece dentro de la esencia del control un indicador de éxito en las operaciones y un sensor que se activa cuando las cosas se desvían en cierta medida de lo correcto.

Una vez identificados los requerimientos de seguridad, deben seleccionarse e implementarse controles para garantizar que los riesgos sean reducidos a un nivel aceptable.

Dentro del marco general de los controles se pueden establecer por lo menos cuatro tipos de controles clasificados por la naturaleza de los mismos y se detallan en la tabla 5.1.

Tipo de control	Cuando se ejecuta?
Correctivo	Una vez que se ha detectado algún fallo.
Preventivo	Una vez detectada la debilidad y diagnosticada la solución.
Compensatorio	Cuando se detecta la debilidad de un control y se implanta otro para cubrir lo que el control originalmente establecido no abarca.
Predictivo	Permiten avizorar los posibles efectos de las debilidades y establecer acciones para prevenirlo.

Tabla 5.1.- Diferentes tipos de controles.

El concepto de riesgo y control esta muy ligado entre sí y se debe tener claro que cada control busca minimizar el efecto de la 'explosión' o materialización de un determinado riesgo, teniendo claro lo anterior se puede establecer la necesidad de que los controles cubran de manera aceptable al riesgo, aunque se podría decir: **"Por que el control no cubre completamente al riesgo?"**. La respuesta a la pregunta anterior es: todo proceso de negocio posee un nivel de riesgo denominado riesgo inherente que esta dentro del proceso del negocio, la única forma de evitar el riesgo inherente es no realizando algún proceso y por obvias razones eso no podría darse ya que se acabaría el negocio y tenemos claro que ese no es el objetivo de un SGSI.

Los riesgos que necesiten ser controlados según los criterios que establezca la gerencia, el nivel que se desee cubrir de los mismos y el costo que implica implementar uno o varios controles a dichos procesos

para lograr establecer una adecuada relación costo-beneficio que permita obtener un resultado positivo en el hecho de establecer controles.

Además se debe considerar que aunque no se puede establecer un porcentaje o cantidad adecuada de controles que debieran implementarse por la diversidad de procesos y sectores en la industria lo que si es muy aconsejable es no asfixiar al proceso con una cantidad exagerada de controles si son no muy necesarios ya que se podría atentar contra el propio negocio y entorpecer los procesos de negocio.

5.2 Controles determinados para los riesgos severos

La siguiente tabla resume los riesgos determinados en el análisis de riesgos, con los respectivos controles de la norma ISO 17799:2005.

Dominio	
5. Política de Seguridad	
Objetivo de Control	
5.1 Política de Seguridad de la Información	
Riesgo	Exista una política de seguridad de la información que no ha sido conocida por todo el personal.
Consecuencia	Los miembros de la organización no conocen de la preocupación de la alta gerencia en materia de seguridad de la información. Pueden darse pérdidas de información valiosa al negocio produciendo la respectiva pérdida financiera.
Controles aplicables	
8.2.2 Conocimiento, educación y entrenamiento de la seguridad de la información.	Todos los empleados de la organización y, cuando sea pertinente, los usuarios externos, deben recibir una adecuada capacitación y actualizaciones periódicas en materia de políticas y procedimientos de la organización.
5.1.1 Documentación de la política de seguridad de la información.	Los responsables del nivel gerencial deben aprobar y publicar un documento que contenga la política de seguridad y comunicarlo a todos los empleados, según corresponda. Éste debe poner de manifiesto su compromiso y establecer el enfoque de la organización con respecto a la gestión de la seguridad de la información.
5.1.2 Revisión de la política de seguridad de la información	La política debe tener un propietario que sea responsable del mantenimiento y revisión de la misma de acuerdo con un proceso definido. Ese proceso debe garantizar que se lleve acabo una revisión en respuesta a cualquier cambio que pueda afectar la base original de evaluación de riesgos
Sugerencias	Talleres de: "difusión a toda la comunidad institucional", de la política de seguridad de la información una vez que esta sea establecida, y aprobada por las autoridades pertinentes.
Riesgo	Existe una política de seguridad desactualizada.

Consecuencia	La seguridad de la información se considera un tema que no preocupa a la alta gerencia y puede producir que sea descuidada con las consecuencias siguientes.

Controles aplicables	
5.1.2 Revisión de la política de seguridad de la información.	La política debe tener un propietario que sea responsable del mantenimiento y revisión de la misma de acuerdo con un proceso definido. Ese proceso debe garantizar que se lleve acabo una revisión en respuesta a cualquier cambio que pueda afectar la base original de evaluación de riesgos
6.1.1 Comité de administración de la seguridad de la información	Debe tenerse en cuenta la creación de un comité gerencial para garantizar que existe una clara dirección y un apoyo manifiesto de la gerencia a las iniciativas de seguridad. Este comité debe promover la seguridad dentro de la organización mediante un adecuado compromiso y una apropiada reasignación de recursos.

Sugerencias	Revisión sistemática de la política de seguridad y ajuste de la misma a los requisitos que se presentaren.

Objetivo de Control	
5.2 Documentación de la política de seguridad de la información	
Riesgo	No contar con políticas y procedimientos respaldos y de recuperación de información.
Consecuencia	El personal no tiene la capacidad para actuar bajo ciertas condiciones en el caso que sucedan incidentes de seguridad

Controles Aplicables	
5.1.1 Documentación de la política de seguridad de la información	Los responsables del nivel gerencial deben aprobar y publicar un documento que contenga la política de seguridad y comunicarlo a todos los empleados, según corresponda. Éste debe poner de manifiesto su compromiso y establecer el enfoque de la organización con respecto a la gestión de la seguridad de la información.
5.1.2 Revisión de la política de seguridad de la información.	La política debe tener un propietario que sea responsable del mantenimiento y revisión de la misma de acuerdo con un proceso definido. Ese proceso debe garantizar que se lleve acabo una revisión en respuesta a cualquier cambio que pueda afectar la base original de evaluación de riesgos
10.1.1 Procedimientos operativos documentados	Se deben documentar y mantener los procedimientos operativos identificados por su política de seguridad. Los procedimientos operativos deben ser tratados como documentos formales y los cambios deben ser autorizados por el nivel gerencial.

Sugerencias	Documentación de políticas y procedimientos que aseguren se pueda recuperar la información en caso de que se requiera. Revisión y evaluación de la política de forma regular.

Tabla 5.2 Controles para los riesgos del dominio Política de seguridad

Dominio	
6. Organización de la Seguridad de la Información	
Objetivo de Control	
6.1 Organización Interna	
Riesgo	No existen procedimientos / controles para modificación del software.
Consecuencia	Pueden darse modificaciones no autorizadas e inescrupulosas a las aplicaciones existentes.
Controles aplicables	
12.5.1 Procedimientos de control de cambios	Debe existir un control estricto de la implementación de los cambios. Se debe imponer el cumplimiento de los procedimientos formales de control de cambios.
12.5.2 Revisiones técnicas de aplicaciones después de operaciones de cambios al sistema	Periódicamente es necesario cambiar el sistema operativo. Cuando se realizan los cambio, los sistemas de aplicación deben ser revisados y probados para garantizar que no se produzca un impacto adverso en las operaciones o en la seguridad.
Sugerencias	Diseño e implementación de procedimientos y controles que aseguren la buena administración de cambios al software.
Riesgo	No existen procedimientos de respaldo.
Consecuencia	Pérdidas de información en elementos que respaldan la misma.
Controles aplicables	
10.1.1 Procedimientos operativos documentados	Se deben documentar y mantener los procedimientos operativos identificados por su política de seguridad. Los procedimientos operativos deben ser tratados como documentos formales y los cambios deben ser autorizados por el nivel gerencial.
10.5.1 Información de respaldos	Se deben realizar periódicamente copias de resguardo de la información y el software esenciales para la empresa. Se debe contar con adecuadas instalaciones de resguardo para garantizar que toda la información y el software esencial de la empresa pueden recuperarse una vez ocurrido un desastre o falla de los dispositivos.
Sugerencias	Diseño e implementación de procedimientos de respaldo adecuado en tecnología y costos para la información critica de ESPOL contenida en sus computadores centrales. Asignación de responsabilidades para el procedimiento de respaldo.

Riesgo	No existen procedimientos de recuperación.
Consecuencia	Pérdida definitiva de información crítica para la organización

Controles aplicables	
10.1.1 Procedimientos operativos documentados	Se deben documentar y mantener los procedimientos operativos identificados por su política de seguridad. Los procedimientos operativos deben ser tratados como documentos formales y los cambios deben ser autorizados por el nivel gerencial.
10.5.1 Información de respaldos	Se deben realizar periódicamente copias de resguardo de la información y el software esenciales para la empresa. Se debe contar con adecuadas instalaciones de resguardo para garantizar que toda la información y el software esencial de la empresa pueden recuperarse una vez ocurrido un desastre o falla de los dispositivos.

Sugerencias	Diseño e implementación de procedimientos de recuperación adecuados en tecnología y costos para la información critica de ESPOL contenida en sus computadores centrales. Asignación de responsabilidades para procedimientos de recuperación de información.

Riesgo	No tener documentación adecuada que respalde las operaciones realizadas.
Consecuencia	En el caso de alguna operación fraudulenta no se tendrían las fuentes para determinar la causa ni el culpable.

Controles aplicables	
10.1.1 Procedimientos operativos documentados	Se deben documentar y mantener los procedimientos operativos identificados por su política de seguridad. Los procedimientos operativos deben ser tratados como documentos formales y los cambios deben ser autorizados por el nivel gerencial.
10.10.3 Protección de la información del log	El log debe ser debidamente protegido y revisado.
10.10.4 Administración y operación de logs	Los logs deben ser administrados y revisados periódicamente.

Sugerencias	Diseño e implementación de procedimientos de documentación de las operaciones. Revisión de forma mensual de la documentación de las operaciones de una muestra extraída de las operaciones realizadas. Registro en una bitácora de operaciones las fechas y actividades realizadas.

Riesgo	No se encuentre separada las áreas de desarrollo con la de producción.
Consecuencia	Puede existir manipulación de datos críticos para la organización.

Controles aplicables	
10.1.4 Separación de las facilidades de	La separación entre las instalaciones de

desarrollo y operación	desarrollo, prueba y operaciones es importante para lograr la separación de los roles involucradas. Se deben definir y documentar las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.
Sugerencias	Clasificación de los equipos tecnológicos para las áreas de desarrollo y de producción. Segregación de los medios de desarrollo y operacionales. Establecer un jefe por cada una de las áreas que sea el responsable de autorizar las actividades dentro de su respectiva área.

Tabla 5.3 Controles para los riesgos del dominio organización de la seguridad de la información

Dominio	
11. Control de Accesos	
Objetivo de Control	
11.3 Responsabilidades del usuario	
Riesgo	Uso de software ilegal, no autorizado, pirata o compartido.
Consecuencia	La violación de copyright de software podría ocasionar daños financieros serios a la empresa. Las multas son severas y los procesos legales costosos. Los discos falsificados pueden estar infestados de virus que dañarán su disco duro y pueden inhabilitar su red. El software no autorizado podría ocasionar problemas con la carga de software instalada en los sistemas de los empleados
Controles aplicables	
15.1.2 Derechos de propiedad intelectual.	Se deben implementar los procedimientos adecuados para asegurar los cumplimientos de las restricciones legales sobre uso de material con respecto a derecho de propiedad intelectual y sobre el producto de software propios.
Sugerencias	Revisión periódica de una muestra de equipos de los computadores de ESPOL Concientización a los usuario sobre el uso de software ilegal. Bloqueo a nivel de sistema operativo de permisos de instalación de software en las instalaciones de trabajo
Riesgo	Ingeniería Social.
Consecuencia	La Ingeniería Social es uno de los mayores riesgos a los que se enfrentan hoy en día, este consiste en relaciones interpersonales que buscan conseguir información confidencial a base de engaños para poder causar estafas, fraudes, sabotajes, espionaje, o algún daño a la organización.
Controles aplicables	
8.2.2 Conocimiento, educación y entrenamiento de la seguridad de la información	Todos los empleados de la organización y donde sea relevante, los usuarios de terceras personas deben recibir una capacitación apropiada y se deben actualizar regularmente de las políticas y procedimientos de la organización.
Sugerencias	Concientización de forma continua a los usuarios sobre los riesgos de Ingeniería Social

Objetivo de Control	
11.3 Responsabilidades del usuario	
Riesgo	Spam.
Consecuencia	Daña la infraestructura informática, por un uso inútil de la banda ancha, la denegación de servicio por saturación o la transmisión de virus y gusanos. Afecta la productividad empresarial
Controles aplicables	
8.2.2 Conocimiento, educación y entrenamiento de la seguridad de la información. .	Todos los empleados de la organización y donde sea relevante, los usuarios de terceras personas deben recibir una capacitación apropiada y se deben actualizar regularmente de las políticas y procedimientos de la organización.
Sugerencias	Concientización a los usuario sobre los Spam. Configuración de servidores de mensajes contra "Lista negras" de correos establecidas Uso de un sistema antispam. Definición de filtros para la clasificación de los mensajes recibidos. Uso de dos direcciones de correo electrónico una para cuando el destinatario no sea confiable

Objetivo de Control	
11.1 Requerimientos del negocio para control de acceso	
Riesgo	No se realiza una actualización periódica del software antivirus instalado.
Consecuencia	Se pueden infectar los equipos de computación de algún nuevo virus. Afecta la productividad empresarial
Controles aplicables	
10.1.1 Procedimientos operativos documentados	Se deben documentar y mantener los procedimientos de operación.
10.4.1 Controles contra código malicioso	Se deben establecer controles de detección y prevención para protegerse del software malicioso y se deben implementar procedimientos apropiados de concienciar al usuario.
Sugerencias	Diseño e implementación de procedimientos de uso de software antivirus. Revisión de políticas y procedimientos de uso de software antivirus por lo menos una vez al ano. Educar a los usuarios de modo que presten atención a estas políticas y procedimientos. Forzar la ejecución de las actualizaciones de antivirus en el Log on de usuarios en las computadoras. Para dicho efecto se debería realizar las descargas actualizaciones automáticas desde el servidor sobre los antivirus utilizados.

Riesgo	Imposibilidad de identificar las autorizaciones y motivos de los cambios realizados por Ausencia de pistas de auditorias.
Consecuencia	No poder identificar cambios realizados en los sistemas. No poder detectar culpables de posibles fraudes.
Controles aplicables	
10.10.1 Log de auditoria	
10.10.2 Monitoreo del uso del sistema	

10.10.3 Protección de la información del Log	
10.10.4 Administración y operación de logs	
10.10.5 Fallas de Log	
Sugerencias	Diseño e implementación de pistas de auditorias en las bases de datos, aplicaciones y sistema operativo. Revisión de las pista de auditoria

Objetivo de Control	
11.1 Requerimientos del negocio para control de acceso	
Riesgo	No exista chapas de seguridad eléctrica u otro mecanismo de control de ingreso en el área de servidores.
Consecuencia	Personal no autorizado podría acceder a áreas restringidas y causar sabotajes, robo de información, o daño de equipos.
Controles aplicables	
9.1.1 Seguridad del perímetro físico	La organización debe utilizar perímetros de seguridad para proteger áreas que contienen medios de procesamiento de información
9.1.2 Controles de entrada físicos	Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que solo se permita acceso al personal autorizado.
9.1.3 Seguridad en oficinas, cuartos y ambientes	Se deben crear áreas seguridad para proteger las oficinas, habitaciones y medios con requerimientos de seguridad especiales.
Sugerencias	Implementación de cerraduras de seguridad. Revisión del funcionamiento de las cerraduras de seguridad. Revisión de la cultura del uso de las cerraduras de seguridad.

Riesgo	No se registren los ingresos del personal al centro de cómputo en una bitácora.
Consecuencia	Si se llegase a presentar algún problema como robo, sabotaje, fraude de información o equipo no podría establecerse que personal ingreso ese día al centro de cómputo.
Controles aplicables	
9.1.1 Seguridad del perímetro físico	La organización debe utilizar perímetros de seguridad para proteger áreas que contienen medios de procesamiento de información
9.1.2 Controles de entrada físicos	Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que solo se permita acceso al personal autorizado.
9.1.3 Seguridad en oficinas, cuartos y ambientes	Se deben crear áreas seguridad para proteger las oficinas, habitaciones y medios con requerimientos de seguridad especiales.
Sugerencias	Registros de ingresos al centro de cómputo en una bitácora de ingresos. Revisión diaria de la bitácora de ingreso

Objetivo de Control	
11.1 Requerimientos del negocio para control de acceso	
Riesgo	No se cambie periódicamente códigos de acceso digitales si existiera esta tecnología en el centro de cómputo.
Consecuencia	Los códigos de acceso pueden llegar a ser conocidos por personas mal intencionado y causar algún perjuicio para la organización.
Controles aplicables	
9.1.1 Seguridad del perímetro físico	La organización debe utilizar perímetros de

	seguridad para proteger áreas que contienen medios de procesamiento de información
9.1.2 Controles de entrada físicos	Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que solo se permita acceso al personal autorizado.
9.1.3 Seguridad en oficinas, cuartos y ambientes	Se deben crear áreas seguridad para proteger las oficinas, habitaciones y medios con requerimientos de seguridad especiales.
Sugerencias	Revisión periódica del cambio de códigos de acceso

Riesgo	No exista un responsable de la seguridad del acceso físico al centro cómputo.
Consecuencia	No contar con un responsable que sea el encargado de la seguridad del acceso físico del centro de cómputo por tal razón se correría un riesgo alto de algún sabotaje, robo, o destrucción de información confidencial o equipo de computación.
Controles aplicables	
6.1.3 Asignación de responsabilidades de seguridad de la información	Se deben definir claramente las responsabilidades para la protección de los activos.
9.1.2 Controles de entrada físicos	Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que solo se permita acceso al personal autorizado.
Sugerencias	Establecer un responsable de la seguridad física del centro de cómputo. Guardias de Seguridad

Objetivo de Control	
9.1 Requerimientos del negocio para el control de accesos	
Riesgo	Que en la política de seguridad no se considere el acceso físico al centro cómputo.
Consecuencia	Dada la importancia de mantener instalaciones seguras dentro de la política debe especificarse claramente las restricciones físicas al centro de cómputo para personas ajenas a las operaciones del mismo.
Controles aplicables	
5.1.2 Revisión de la política de seguridad de la información	La política de seguridad de la información debe contener claramente las restricciones en cuanto a acceso físico al centro de cómputo, si no se ha considerado inicialmente o no lo incluye debe extender el alcance e incluir dicho punto.
9.1.1 Se debe restringir el acceso a lo que se defina en la política de control de acceso.	Deben quedar claramente documentado dentro de la política la restricción y la obligatoriedad de cumplimiento de la misma y asegurar su entendimiento.
Sugerencias	Establecer como punto necesario el incluir dentro del texto de la política de seguridad lo relacionado a acceso físico al centro de cómputo.

Riesgo	Exista solo una persona encargada de las llaves del centro de cómputo.
Consecuencia	La existencia de un solo conjunto de llaves para acceder al centro de computo y que solo una persona se encargue de las mismas crea una gran dependencia y fragilidad sobre el acceso al centro de computo, si la

	persona no es muy cumplida o le sucede algo con las llaves seria un gran inconveniente con una solución no muy ágil.
Controles aplicables	
Duplicar el juego de llaves y disponer estas en un lugar seguro, accesible y cercano al centro de cómputo.	Aunque se puede trabajar como se menciona, el hecho de disponer de un duplicado del juego de llaves podría ayudar ante cualquier emergencia sin interrumpir demasiado tiempo las actividades
Sugerencias	Creación de lineamientos para ingreso al centro de computo y dar a conocer las diversas opciones que se tienen para el mismo ya que esto debe ser conocido por todos los que trabajan en el centro de computo y la gerencia de sistemas.
Riesgo	No se encuentre activada el área de log en donde se registre el acceso a los sistemas.
Consecuencia	El desconocimiento de los accesos realizados por los usuarios del sistema al mismo o la imposibilidad de identificar posibles autores de fraudes dentro de la compañía o desde fuera de ella.
Controles aplicables	
9.7.1 Activación del diario de eventos	Se debe producir diarios de auditoria que registren las excepciones, accesos a los sistemas y las operaciones realizadas dentro de los sistemas y se deben mantener durante un periodo acordado para ayudar en investigaciones futuras y monitorear el control de acceso.
Sugerencias	Debe designarse al encargado de que todos los registros sean almacenados en el log, y deben revisarse de forma periódica dichos registros, el encargado debe evidenciar el cumplimiento de dicha actividad con informes o verificaciones de las actividades relevantes o hallazgos obtenidos y debidamente reportarlos a la alta gerencia.
Riesgo	No exista el personal encargado de la revisión del área de log de acceso al sistema.
Consecuencia	En el caso de haberse efectuado algún crimen o fraude, se tendría la evidencia en el log de la operación fraudulenta y no seria detectada ya que nadie revisa dicho log, es muy similar a que si no se llevara dicho registro.
Controles aplicables	
10.10.3 Protección de la información del log	El log debe ser debidamente protegido y revisado.
10.10.4 Administración y operación de logs	Los logs deben ser administrados y revisados periódicamente.
Sugerencias	Registro en una bitácora de operaciones las fechas y actividades realizadas. Establecimiento de un debido procedimiento de reporte de hallazgos en los logs de registros de acceso y actividad en el sistema
Riesgo	No exista un mecanismo adecuado que valide el acceso a los sistemas desde la parte externa (Confirmación de llamada, verificación de la redundancia).
Consecuencia	Podría haberse clonado una estación remota y se realiza la llamada desde otro numero o dirección y de no verificarse podría ser la puerta abierta a

	facturas ficticias, ventas no realizadas pero si registradas, entre otros.
Controles aplicables	
9.4.3 Autenticación de nodo	Se deben autenticar las conexiones a sistemas de cómputo remotos.
9.4.3 Autenticación del usuario para conexiones externas	El acceso de usuarios remotos debe estar sujeto a autenticación.
Sugerencias	Tener identificadores de llamadas remotas y validar contra la lista de direcciones autorizadas. Se debe conocer cualquier cambio en las conexiones externas para validar dicha entrada y no interrumpir el negocio.
Riesgo	Las aplicaciones o programas solo interactúen con lo necesario de la base de datos más no con el total de la misma.
Consecuencia	Dar acceso al total de la base de datos podría ser muy peligroso en el caso de que se quieran cometer un delito, el manejo de usuarios tipo administrador para aplicaciones que no necesitan dicho privilegio ya que solo registran transacciones, consultan o ambas ya que se podría tener acceso con las herramientas adecuadas a el total de la base de datos y se podría modificar los registros de transacciones hechas por los usuarios por citar un ejemplo.
Controles aplicables	
9.4.3 Autenticación de nodo	Se deben autenticar las conexiones a sistemas de cómputo remotos.
9.4.3 Autenticación del usuario para conexiones externas	El acceso de usuarios remotos debe estar sujeto a autenticación.
Sugerencias	Los usuarios de acceso a la base de datos deben estar claramente identificados para poder asignar responsabilidades directas en la interacción de los usuarios con los sistemas.

Tabla 5.4 Controles para los riesgos del dominio Control de accesos

5.3 Propuesta de implementación de controles

Como parte final del presente trabajo, proponemos un cronograma de implementación para los controles establecidos para mitigar los riesgos identificados en los objetivos de control.

La tabla 5.5 muestra el plan de trabajo a 2 años dividido por semestres y la tabla 5.6 muestra el plan de trabajo dividido por meses durante los 2 años de implementación propuestos.

Tabla 5.5 Propuesta de implementación por semestres

IMPLEMENTACION DE CONTROLES POR SEMESTRE				
Control	**Semestre**			
	Semestre I	**Semestre II**	**Semestre III**	**Semestre IV**
5.1.1 Documentación de la política de seguridad de la información.	x			
5.1.2 Revisión de la política de seguridad de la información			x	
6.1.1 Comité de administración de la seguridad de la información	x			
6.1.3 Asignación de responsabilidades de seguridad de la información	x			
8.2.2 Conocimiento, educación y entrenamiento de la seguridad de la información.	x	x	x	
9.1.1 Seguridad del perímetro físico		x		
9.1.2 Controles de entrada físicos	x	x		
9.1.3 Seguridad en oficinas, cuartos y ambientes		x		
9.1.4 Protección contra amenazas externas		x		
9.1.5 Trabajo en áreas seguras			x	
10.1.1 Procedimientos operativos documentados	x	x		
10.1.4 Separación de las facilidades de desarrollo y operación		x	x	
10.4.1 Controles contra código malicioso		x	x	
10.5.1 Información de respaldos		x	x	
10.10.1 Log de auditoria			x	
10.10.2 Monitoreo del uso del sistema			x	x
10.10.3 Protección de la información del log			x	x
10.10.4 Administración y operación de logs			x	x
10.10.5 Fallas de log				x
11.1.1 Política de control de acceso	x			
11.5.2 Identificación y autenticación de usuario	x			
12.2.2 Control de procesamiento interno		x	x	
12.5.1 Procedimientos de control de cambios		x		
12.5.2 Revisiones técnicas de aplicaciones después de operaciones de cambios al sistema			x	x
15.1.2 Derechos de propiedad intelectual	x			

Tabla 5.6 Propuesta de implementación por meses

IMPLEMENTACION DE CONTROLES POR MESES																								
Control	Semestre I						Semestre II						Semestre III						Semestre IV					
	Mes						Mes						Mes						Mes					
	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6
5.1.1 Documentación de la política de seguridad de la información.	x	x	x	x	x	x																		
5.1.2 Revisión de la política de seguridad de la información													x	x										
6.1.1 Comité de administración de la seguridad de la información	x																							
6.1.3 Asignación de responsabilidades de seguridad de la información		x	x																					
8.2.2 Conocimiento, educación y entrenamiento de la seguridad de la información.				x	x	x	x	x									x	x						
9.1.1 Seguridad del perímetro físico							x	x	x															
9.1.2 Controles de entrada físicos						x	x	x																
9.1.3 Seguridad en oficinas, cuartos y ambientes								x	x															
9.1.4 Protección contra amenazas externas									x	x														
9.1.5 Trabajo en áreas seguras															x	x								
10.1.1 Procedimientos operativos documentados							x	x																
10.1.4 Separación de las facilidades de desarrollo y operación									x	x				x	x									
10.4.1 Controles contra código malicioso										x	x	x	x											
10.5.1 Información de respaldos										x	x	x	x	x										
10.10.1 Log de auditoria												x	x	x	x	x	x							
10.10.2 Monitoreo del uso del sistema														x	x	x	x	x	x					
10.10.3 Protección de la información del log																x	x	x	x	x	x			
10.10.4 Administración y operación de logs																		x	x	x	x	x	x	
10.10.5 Fallas de log																			x	x	x	x	x	x
11.1.1 Política de control de acceso			x	x																				
11.5.2 Identificación y autenticación de usuario	x	x	x																					
12.2.2 Control de procesamiento interno									x	x	x	x	x											
12.5.1 Procedimientos de control de cambios										x	x	x												
12.5.2 Revisiones técnicas de aplicaciones después de operaciones de cambios al sistema														x	x	x							x	x
15.1.2 Derechos de propiedad intelectual	x	x	x																					

CAPITULO 6

6 Conclusiones y recomendaciones

6.1 Conclusiones

- La seguridad de la información se ha convertido actualmente en una de las mayores preocupaciones de las organizaciones debido a que la información es un activo crítico cuyo riesgo de pérdida podría llevar a soportar muchas consecuencias negativas para la organización, como pérdidas financieras, pérdida de imagen o inclusive la quiebra.

- La seguridad de la información es una medida para incrementar el éxito de los negocios. El implementar un Sistema de Gestión de la Seguridad de la Información, tal como el que plantea la norma ISO 17799, puede ayudar que una organización cumpla favorablemente los incentivos de mercadotecnia, los financieros y las preocupaciones de empeño para ayudar a lograr oportunidades de crecimiento.

- La norma ISO 17799 proporciona una base para un Sistema de Gestión de la Seguridad de la Información, de forma tal que se puede aplicar a cualquier requisito de Seguridad de la Información, y debe ser ajustable a futuros reglamentos y requisitos.

- Un Sistema de Gestión de Seguridad de la Información brinda una metodología para la administración de los riesgos que pueden afectar la información de una organización.

- Un Sistema de Gestión de Seguridad de la Información se basa en el ciclo Planificar, Hacer, Verificar, Actuar que permite mantener un proceso de mejora continua del sistema, brindando una seguridad razonable que los riesgos que pueden afectar a la seguridad de la información, pueden ser administrados de manera eficiente en todo momento.

- ESPOL como organización no está libre de ataques que comprometan la seguridad de la información y de las debidas consecuencias que éstas podrían ocasionar.

6.2 Recomendaciones

- Se recomienda que durante todas las fases del Sistema de Gestión de Seguridad de la Información se cuente con el apoyo correspondiente por parte de las altas autoridades de ESPOL y del personal a su cargo.

- Concienciar a todos los miembros de la comunidad politécnica sobre la importancia de la seguridad de la información.

- Se recomienda que en las próximas promociones del Diplomado de Auditoria Informática se continúe con el trabajo de diseño del Sistema de Gestión de Seguridad de la Información para ESPOL, ampliando el alcance del mismo y reportar los resultados del trabajo a las debidas autoridades de ESPOL, así como a la Dirección del Centro de Servicios Informáticos de ESPOL.

- Es importante que las autoridades de ESPOL, en el caso de adoptar éste y futuros trabajos de diseño del Sistema de Gestión de Seguridad de la Información para su implementación, realicen previamente una revisión del análisis de riesgos debido a que éstos cambian constantemente y puedan presentarse nuevos riesgos que no existían durante la realización del presente trabajo o de otros que se realicen en el futuro.

- Se recomienda realizar un cronograma detallado para la implementación de los controles determinados durante el desarrollo del presente trabajo, basado en la propuesta de implementación que se encuentra en el capítulo 5.

- Se recomienda una constante evaluación del Sistema de Gestión de Seguridad de la Información mediante auditorias externas, las cuales forman parte de la metodología de implementación que se ha hablado en éste trabajo.

- En el ***ANEXO 15.- Funciones recomendadas para la implementación del sistema de gestión de la seguridad de la información*** se describen los roles que se recomiendan establecer al momento de implementar el SGSI para ESPOL.

BIBLIOGRAFIA

Libros:

1. Manual de Preparación al examen CISA 2005 – Information System audit. And Control Association ISACA

2. Sistemas de información para la gestión empresaria. Procedimientos, seguridad y auditoria – Alberto R. Lardent – Prentice Hall

Documentos:

1. Módulo 1 - Academia Latinoamericana de Seguridad Informática – Microsoft

2. Módulo 2 - Academia Latinoamericana de Seguridad Informática – Microsoft

3. Módulo 3 - Academia Latinoamericana de Seguridad Informática – Microsoft

4. Módulo 4 - Academia Latinoamericana de Seguridad Informática – Microsoft

5. Módulo 5 - Academia Latinoamericana de Seguridad Informática – Microsoft

6. Norma ISO 17799:2000 – International Standards Organization

7. Proyecto de Autoevaluación Institucional - ESPOL

8. CSI/FBI Computer Crime and Security Survey-2004 - Computer Security Institute/ Federal Bureau of Investigation

9. Módulo 1 – Diplomado de Auditoria Informática: Material de estudio – Centro de Educación Continua

10. Módulo 4 – Diplomado de Auditoria Informática: Material de estudio – Centro de Educación Continua

11. Sistemas de administración de riesgos en tecnología informática – Alberto Cancelado

12. Sistemas de administración de riesgos - Alberto Cancelado

13. Gestión de la Seguridad de la Información – Antonio Villalón Huerta -Universidad de Verano Campusti Ciencia y Tecnología

14. Introducción a la seguridad informática parte de la cultura del control – Carlos A. Gros - Bossio Gros & Asociados

15.¿Qué es la norma ISO 17799? – BSI Management System

16.Brochure ISO 17799 - BSI Management System

Enlaces de Internet:

1. www.espol.edu.ec
2. www.isaca.org
3. www.bsi-global.com
4. www.dynamoo.com/orange/
5. www.commoncriteriaportal.org
6. www.sans.org
7. www.iso.org
8. http://www.s21sec.com/s21sec/ser_iso.jsp
9. http://17799.denialinfo.com/index.htm
10. http://www.iso27001security.com/html/iso270001.html
11. www.gocsi.com
12. www.gesteopolis.com
13. http://pwp.etv.net.co/acancelado
14. www.bsiamerica.com/mexico

GLOSARIO

Actividades.- Son las acciones de carácter económico, administrativo y de producción ejecutada en la empresa, normalmente involucrada en procesos decisorios dirigidos a alcanzar los objetivos de la organización. Su identificación sirve de base para el mejoramiento de la gestión y su evaluación permanentemente, con el objeto de mejorar la marcha de la organización.

Activos.- Es todo aquel elemento que compone el proceso de la comunicación partiendo desde la información, emisor, el medio por el cual se transmite hasta su receptor.

Amenazas.- Son agentes capaces de explotar los fallos de seguridad que se denominan puntos débiles y como consecuencia de ello causar pérdidas o danos a los activos de una empresa afectando su negocio.

Análisis de Riesgo.- Es un método de análisis cualitativo donde se considera la estimación de pérdidas potenciales. Para ello se interrelacionan cuatro elementos principales: las amenazas, por definición siempre presentes en cualquier sistema, las vulnerabilidades, que potencian el efecto de las amenazas, el impacto asociado a una amenaza, que indica los daños sobre un activo por la materialización de dicha amenaza, y los controles o salvaguardas, contramedidas para minimizar las vulnerabilidades.

Cerraduras Biométricas.- Cerraduras de puertas y de entradas que son activadas por características biométricas como por ejemplo la voz, la retina del ojo.

Confidencialidad.- Protección de la información de los clientes y de la empresa.

Controles.- Medios por los cuales se alcanzan los objetivos de control.

Declaración de aplicabilidad.- La Declaración de la Aplicabilidad es un documento el cual tiene como objetivo proporcionar la justificación para la aplicabilidad o no aplicabilidad de cada control de la norma ISO 17999 al Sistema de Gestión de Seguridad de la Información en cuestión.

Disponibilidad.- Se refiere a la disponibilidad de la información y de toda la estructura física y tecnológica que permita el acceso, transito y almacenamiento.

Divulgación.- Publicar, extender, poner al alcance del público algo.

Espionaje.- Actividad dedicada a obtener información fraudulenta en diversos campos.

Estándar.- Que sirve como tipo, modelo, norma, patrón o referencia.

Exposición.- Un resultado o consecuencia potencialmente adversa a ser considerada al evaluar los controles internos .Fortalecer los controles internos puede reducir la exposición pero rara vez la elimina.

Firewall.- Es un dispositivo que hace valer políticas de seguridad para el tráfico que atraviesa hacia y desde segmentos diferentes de red.

Hacker.- Persona con altos conocimientos sobre el funcionamiento interno de un sistema, de un ordenador o de una red de ordenadores. Este término se suele utilizar indebidamente como peyorativo, confundiéndolo con el término cracker.

Hardware.- Se refiere a las características técnicas y físicas de la computación.

Ingeniería Social.- Se refiere a la acción de engañar a un usuario para que sea él el que actúe, ejecutando un archivo o revelando datos secretos como una clave. Se utiliza la astucia para convencer a una persona a dar por si mismo información acerca de su sistema.

Integridad.- Una información integra es una información que no ha sido alterada de forma indebida o no autorizada.

Log/registro.- Anotación de los detalles de información o eventos, que se mantienen en un sistema organizado de registro, usualmente secuenciado en el orden en que ocurrieron los hechos.

Materialidad.- Un concepto de auditoria que se refiere a la importancia de un evento de información respecto a su impacto o a su efecto sobre el funcionamiento de la entidad que esta siendo auditada. Una expresión de la significación o importancia relativa de un asunto en particular en el contexto de la organización como un todo.

Plan de Trabajo.- Documento que detalla los recursos y la metodología que se utilizarán en la realización de una evaluación.

Política de Seguridad.- Es una medida que busca establecer los estándares de seguridad a ser seguidos por todos los involucrados en el uso y mantenimiento de los activos.
Es una forma de suministrar un conjunto de normas internas para guiar la acción de las personas en la realización de su trabajo. Es el primer paso para aumentar la conciencia en la seguridad de las personas, pues esta orientada hacia la formación de hábitos por medios de manuales de instrucción y procedimientos operativos.

Procedimiento.- Los documentos de procedimiento brindan información sobre la manera de cumplir con los estándares cuando se esta realizando un trabajo, pero no se fijan los requisitos.

Proceso de Certificación.- Un proceso de certificación consiste en la generación de un informe firmado por parte de un organismo externo, es decir, ajeno a la organización que define que, de acuerdo con su criterio profesional, la organización cumple o no cumple con los requerimientos establecidos en la norma.

Procesos.- Conjuntos de actividades que transforman entradas en salidas, datos en información y aportan valor.

Redes.- Son sistemas de computadoras interconectadas y el equipo de comunicación usado para conectarlas.

Respaldo.- Archivos, equipos, datos, y procedimientos disponibles para su uso en el caso de una falla o perdida, si se destruyen los originales o si se esta en el sitio alterno.

Riesgo de Fraude.- El riesgo de que las actividades incluyan la omisión deliberada de los controles con la intención de ocultar las irregularidades perpetradas, incluyendo el uso no autorizado de activos o de servicios y la tolerancia de los mismos o ayudar a ocultar este abuso.

Riesgo inherente.- El riesgo de que podría ocurrir un error material, asumiendo que no hay controles relacionados para prevenir o para detectar el error.

Riesgos.- El potencial de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y que ocasione perdida de los activos o daños a los mismos. Usualmente se mide mediante la combinación del impacto y de la probabilidad de que ocurra.

Sabotaje.- Daño o deterioro que en las instalaciones, productos, etc., se hace como procedimiento de lucha contra los patronos, contra el Estado o contra las fuerzas de ocupación en conflictos sociales o políticos.

Segregación de funciones.- Es un control básico que impide o que detecta los errores y las irregularidades asignando responsabilidades de iniciar las transacciones, registrar las transacciones y custodiar los activos a personas separadas.

Vulnerabilidad.- Son los elementos que al ser explotados por amenazas afectan la confidencialidad, disponibilidad e integridad de información de un individuo o empresa.

Evidencia.- La información que recoge un auditor en el curso de realización de una auditoria de sistemas de información.

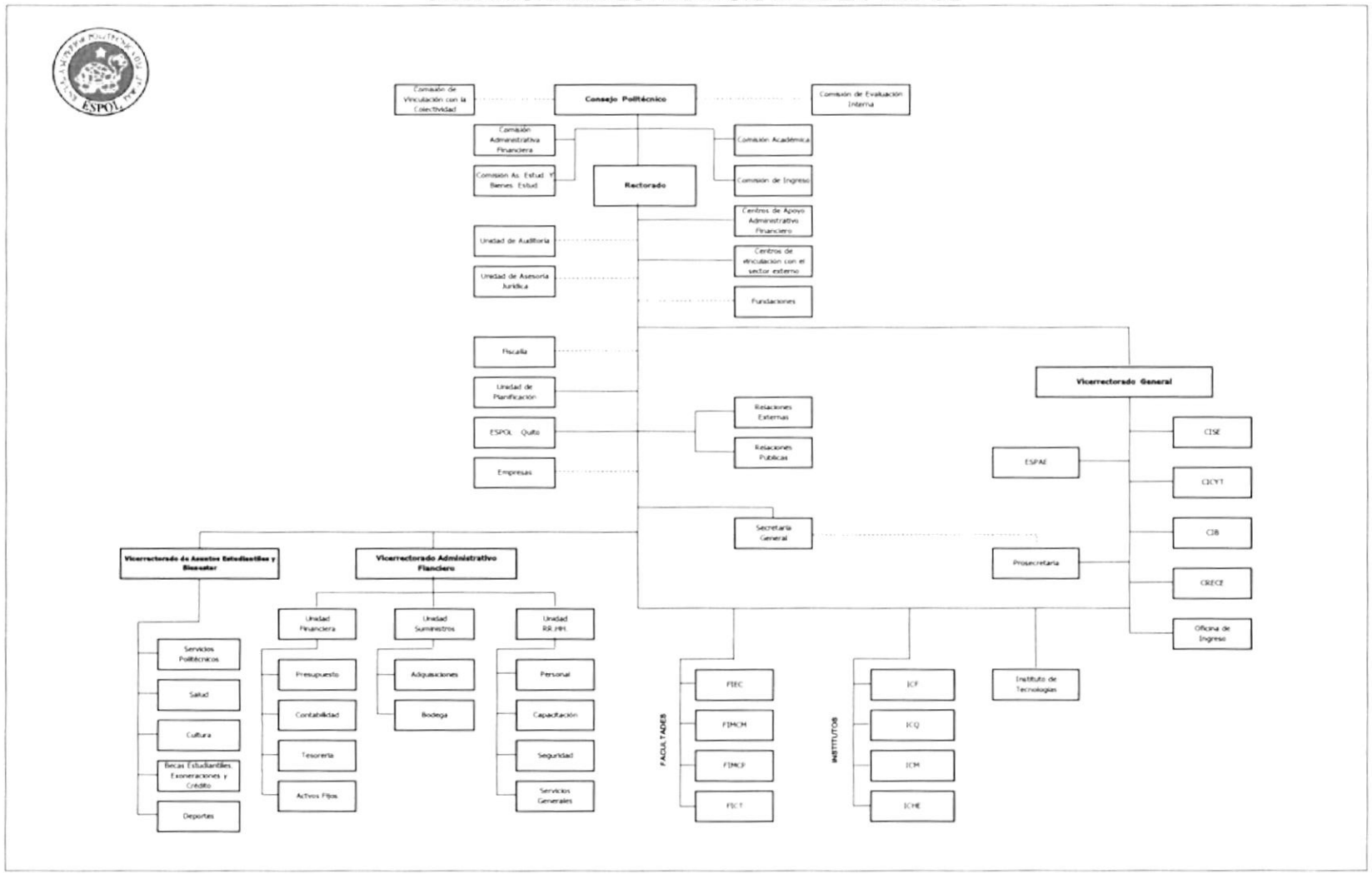
ANEXOS

ANEXO 1.- Organigrama Estructural de ESPOL
ANEXO 2.- Funciones básicas centros y unidades de ESPOL
ANEXO 3.- Plan estratégico ESPOL 2004-2007
ANEXO 4.- Entrevistas autoridades ESPOL
ANEXO 5.- Descripción de Sistemas Financiero y Académico ESPOL
ANEXO 6.- Inventario de Hardware ESPOL
ANEXO 7.- Inventario de Software ESPOL
ANEXO 8.- Documentos y formularios
ANEXO 9.- Índice de manuales
ANEXO 10.- Organigrama CSI –ESPOL
ANEXO 11.- Funciones y responsabilidades del personal del CSI
ANEXO 12.- Inventario de riesgos
ANEXO 13.- Asignación de Probabilidad vs. Impacto a riesgos aplicables
ANEXO 14.- Ejemplo Carta de certificación Banco de Montreal
ANEXO 15.- Funciones recomendadas para la implementación del Sistema de Gestión de Seguridad de la Información en ESPOL

Anexo 1

Organigrama estructural de la ESPOL

ORGANIGRAMA ESTRUCTURAL DE LA ESPOL



Anexo 2

Funciones básicas de los centros y unidades de la ESPOL

FUNCIONES BÁSICAS DE LOS DIFERENTES CENTROS Y UNIDADES DE LA ESPOL

ORGANISMOS Y UNIDADES ADMINISTRATIVAS DE LA ADMINISTRACIÓN CENTRAL

UNIDAD	FUNCIÓN BÁSICA
Consejo Politécnico	Resolver asuntos correspondientes al Rector y Vicerrectores; Proponer reformas al estatuto; Aprobar anualmente Planes Estratégicos y Operativos, Presupuestos y Reglamentos de la Institución; Aprobar planes y programas de estudios, nombramiento de profesores, creación o suspensión de unidades; Evaluar los resultados obtenidos en base a metas acordadas y tomar medidas de reajuste necesarias.
Comisión Vinculación con la Colectividad	Fomentar el proceso permanente de vinculación de la ESPOL con las cámaras de Producción, Organizamos no Gubernamentales, prestigiosas Universidades y Escuelas Politécnicas nacionales y extranjeras y medios de comunicación externos, gobierno y sector productivo en general.
Comisión de Evaluación Interna	Diseñar, coordinar y supervisar procesos, planes y políticas de autoevaluación y acreditación. Determinar dimensiones, criterios, características e indicadores de calidad. Evaluar cumplimiento de planes y políticas institucionales.
Comisión Académica	Es un organismo de soporte del Consejo Politécnico, el cual está conformado por miembros de éste último organismo y asesora en asuntos relacionados con las actividades académicas de la ESPOL. La preside El Vicerrector General.
Consejo de Postgrado	Planificar, controlar y recomendar políticas y programas de postgrado al Consejo Politécnico
Rectorado	Convocar y presidir el Consejo Politécnico; Cumplir y hacer cumplir las leyes, estatutos, reglamentos, acuerdos y resoluciones del Consejo Politécnico; Velar por la correcta recaudación de las rentas; Autorizar y legalizar gastos y contratos no planificados; Extender nombramientos, celebrar contratos, conceder licencias a profesores, trabajadores, investigadores y diferentes miembros de la Institución; Procurar el incremento de los bienes de la ESPOL; Autorizar publicaciones; Proponer al Consejo Politécnico la política y lineamientos generales de la ESPOL.
Unidad de Auditoria	Supervisa y audita las actividades para que los recursos de la ESPOL sean bien utilizados.

Centros de Apoyo Administrativo Financiero	Encargados de dar apoyo al rectorado en el manejo de proyectos institucionales y de las unidades académicas, vinculados con el sector productivo. Existe también un centro encargado de la inserción estudiantil al sector productivo.
Unidad de Asesoría Jurídica	Absolver las consultas jurídicas presentadas por organismos, autoridades y jefes de dependencias administrativas, patrocinando acciones de defensa de la Institución. Asesorar y elaborar reformas a los reglamentos, acuerdos y resoluciones internas, elaborar y revisar contratos y convenios, emitir criterios legales en relación a los aspectos jurídicos que se le consulten, coordinar y coadyuvar la información sumaria que surgiera contra algún miembro de la comunidad, patrocinar a la ESPOL en los juicios y mas trámites judiciales ya sea como actora o demandada.
Centros de vinculación con colectividad	Son organismos encargados de administrar formular e implementar proyectos que demanda el sector productivo. Así como existen centros encargados de desarrollar y transferir tecnología al sector productivo.
Fundaciones	Son organismos creados para desarrollar investigación o desarrollar tecnología conjuntamente administrados con el sector productivo. Otras fundaciones operan con la finalidad de facilitar la administración de ciertas actividades que desarrolla la ESPOL y que dada la complejidad de ciertas actividades se necesita de la estructura de una fundación para poder cumplir con eficacia los objetivos establecidos en esa actividad en particular.
Empresas	Son organizaciones creadas bajo la modalidad de subsidiaria propia o de contratos de asociación con el sector empresarial, con la finalidad de realizar investigación o desarrollo de tecnologías o también son entes creados bajo la modalidad de una empresa con la finalidad de dar un apoyo eficiente y ayuden a autofinanciar los servicios que requiere la ESPOL
Fiscalía	Garantizar y súper vigilar que en los trámites administrativos, académicos , investigación y juzgamiento administrativo se cumplan de acuerdo al estatuto, reglamentos y disposiciones de la ESPOL, absolver las consultas realizadas por unidades y organismos de la ESPOL.
Unidad de Planificación	Planificar y Coordinar el desarrollo de la Infraestructura física Institucional y dar soporte para la formulación e implementación del Plan Estratégico de la ESPOL
ESPOL-Quito	Oficina encargada de dar apoyo administrativo y académico de las actividades que realiza la ESPOL en la ciudad de Quito.
Relaciones Externas	Propiciar las relaciones con centros universitarios nacionales y extranjeros, fortalecer los vínculos ya existentes con los mismos, coordinar y legalizar la concesión de becas, supervisar el cumplimiento de los programas de estudios que deben seguir los becarios, controlar el cumplimiento de las obligaciones contractuales de los beneficiarios para con la Institución en los diferentes

	planes y programas de ayuda de estudios. Canalizar las propuestas y proyectos de ayuda y cooperación internacional y nacional, convenios y compromisos de cooperación.
Relaciones Públicas	Oficina encargada de difundir internamente y externamente las actividades que realiza la ESPOL a través de la producción de material gráfico, audiovisual y documental , organizar y ejecutar los actos públicos institucionales en el área de su competencia, mantener relaciones públicas con los sectores políticos, económicos, científicos y sociales sobre asuntos que son de interés institucional; y mantener archivos informáticos de: recortes de prensa, fotografías , boletines informáticos, afiches, documentales y demás publicaciones relacionadas con la ESPOL
Secretaría General	Dar asistencia a los organismos, extender certificados y legalizar documentos institucionales, mantener y resguardar el archivo central.

FUNDACIONES

FUNDACIÓN	FUNCIÓN BÁSICA
CENAIM- ESPOL	Administrar las actividades del Centro Nacional de Investigaciones Marinas. El Directorio está conformado por representantes del sector camaronero y autoridades de la ESPOL.
Fundación para el desarrollo de la enseñanza media (FUNDAEM)	Entidad encargada de administrar las actividades del Colegio Politécnico (COPOL). El Directorio está conformado por autoridades de la ESPOL
Fundación para el desarrollo de la ESPOL (FUNDESPOL)	Organismo encargado de administrar y dar apoyo administrativo a las unidades que operan en el Campus Las Peñas. El Directorio está conformado por autoridades de la ESPOL
FUNDACIÓN ESPOL 50 AÑOS	Entidad encargada de captar donaciones provenientes del 25 % del impuesto a la renta de personas naturales y jurídicas que operan en el país.

EMPRESAS

EMPRESA	FUNCIÓN BÁSICA
ESPOLTEL	Empresas encargadas de administrar las tecnologías de información, computación y comunicación. La ESPOL posee el 100% de las acciones
Servicios de Biotecnología Compañía Anónima	Empresa dedicada a desarrollar tecnología en el campote la biotecnología

(CEBIOCA)	enfocada principalmente en el banano y caña de azúcar. La ESPOL posee el 20% de las acciones, el resto de acciones la poseen empresarios del sector bananero y cañicultor.
TRANSESPOL	Empresa encargada de administrar el sistema de transporte de la ESPOL para dar servicio a la comunidad, La ESPOL posee el 100% de las acciones.
AGROSAIZA	Empresa encargada de hacer importación de materias primas, siembra, cultivo, fabricación, comercialización de productos agrícolas, especies vegetales, maquinarias, herramientas, repuestos y vehículos para el sector agropecuario y agroindustrial.
EXPOPEZA	Microempresa encargada del Manejo de Cultivos Orgánicos.

CENTROS DE APOYO ADMINISTRATIVO FINANCIERO

CENTRO	FUNCIÓN BÁSICA
Centro de Prestación de Servicios (CPS)	Asesoría y control de gestión financiera de proyectos, promoción de proyectos en coordinación con las unidades académicas y centros de vinculación con la comunidad.
Dentro de Difusión y Publicaciones	Satisfacer las necesidades de diseño, diagramación e impresión y todo lo relacionado con las artes gráficas dentro de la comunidad politécnica y al público en general.
Centro de Servicios Informáticos (CSI)	Administrar el sistema de información de la ESPOL tanto académico, administrativo y financiero.
Centro de Promoción y Empleo (CEPROEM)	Servir de nexo entre los estudiantes de los últimos niveles de las diferentes carreras con empresas de prestigio nacional e internacional, a fin de viabilizar la ubicación de éstos

CENTROS DE VINCULACIÓN CON LA COMUNIDAD

CENTRO	FUNCIÓN BÁSICA
Centros de Estudios del Medio Ambiente (CEMA)	Realizar planes de desarrollo urbano y cantonal, estudio de servicios básicos: Botaderos, mataderos, redes de alcantarillado, sanitario y pluvial, diseño de sistemas de tratamiento de aguas residuales, domésticas e industriales, manejo de desechos sólidos, asistencia técnica de campo con instrumentación ambiental, entrenamiento de personal en prevención y control del medio ambiente. (Prestar

	servicios de análisis y estudios relacionados con el medio ambiente)
Centro de Transferencia y desarrollo de Tecnología (CTDT)	Promover la investigación científica y tecnológica; Propiciar la creación o el mejoramiento de laboratorios, gabinetes u otros medios idóneos para la investigación en los centros de educación superior; establecer y mantener la cooperación de los establecimientos de educación superior con las empresas privadas y públicas nacionales en el desarrollo de tecnologías; colaborar con organismos, instituciones o empresas públicas y privadas extranjeras para la transferencia y adaptación de tecnologías a las necesidades del país; diseñar proyectos de desarrollo, participar en su ejecución y evaluarlos.
Centro de Investigaciones Biotecnológicas del Ecuador (CIBE)	Desarrollar investigación en biotecnología orientado al banano y plátano para la mejora genética para incrementar la resistencia a la sigatoca negra en ambiente sustentable. Estas actividades se realizan en alianza con organismos y universidades internacionales conjuntamente con productores bananeros.
Centro de Tecnologías de la Información (CTI)	Facilitar y fomentar la planificación del uso de tecnologías de información, dentro del aula de clases, además, buscar la absorción, adaptación, innovación y desarrollo de nuevas tecnologías de información para beneficio de una mejor educación tanto dentro como fuera de la ESPOL
Centro de Estudios Arqueológicos y Antropológicos (CEAA)	Desarrollar investigación de los aspectos arqueológicos y antropológicos enfocados al litoral ecuatoriano
Centro de Lenguas Extrajeras (CELEX)	Ofrecer cursos de inglés a los estudiantes de la ESPOL y personal externo, realizar traducciones de todo tipo de documentos económicos, evaluar profesores de inglés de otras instituciones, realizar exámenes de ubicación TOEFL, ofrecer servicios de consultoría académica.(Ofrecer estudios en lenguas extranjeras a los estudiantes de la ESPOL y personal externo.
Centro de Educación Continua (CEC)	Apoyar a las unidades académicas en la organización de cursos, seminarios, conferencias, mesas redondas, etc. Además realiza las mismas actividades con temas de interés general no relacionados con las actividades específicas de cada unidad académica.
Centro de Desarrollo de la productividad y Mejoramiento Continuo (CEDEP)	Ejecutar planes y políticas de capacitación y formación profesional
Centro de Entrenamientos de Emprendedores (CEEMP)	Proveer formación en conocimientos y habilidades, propicia el contexto adecuado y facilita los contactos que permitan a los emprendedores concebir y lanzar negocios exitosos basados en ideas innovadoras.

CENTROS DE APOYO ACADÉMICO

CENTRO	FUNCION BASICA
Centro Nacional de Recursos Costeros (CENAREC)	Desarrollar sistemas de manejo ambiental en la costa ecuatoriana, en la agricultura e impacto ambiental en la población natural de camarones y desarrollo de un sistema de alerta de la acuicultura del camarón a través del uso de un sistema de información geográfica. (GIS)
Centro de Investigaciones Estadísticas (CEIE)	Paralelo con la carrera Ingeniería en Estadística Informática de la ESPOL, funciona el Centro de Estudios e Investigaciones Estadísticas ICM-ESPOL, que tiene, entre otros los siguientes objetivos: Propiciar la ejecución de Consultoría en Estadística Informática, Dar entrenamiento profesional a los Estudiantes, Ofrecer pasantías a estudiantes y profesores, Hacer de la ESPOL un punto de referencia para el Sistema Estadístico Nacional.
Centro de Investigaciones Económicas (CIEC)	EL propósito es generar conocimientos, información, investigación y análisis en materia económica y en gestión de empresas, para satisfacer la demanda y el interés de los sectores productivos y la sociedad en general, propiciando la formación de una cultura de investigación.
Centro de Servicios para la acuicultura (CSA)	Buscar soluciones a las enfermedades del camarón
Centro de Investigaciones Oceánicas y Pesqueras (CIOP)	El objetivo es brindar servicios, tecnología y asesoría al sector pesquero ecuatoriano como un medio de maximizar el desarrollo de las pesquerías, utilizando para ello el conocimiento científico de los procesos oceánicos y atmosféricos que ocurren a diferentes escalas de tiempo y espacio, y sus efectos en los ecosistemas y recursos marinos.
Centro de Investigaciones Biotecnológicas (CIBE)	Desarrollar investigación en biotecnología orientado al banano y plátano para la mejora genética para incrementar la resistencia a la sigatoca negra en ambiente sustentable. Estas actividades se realizan en alianza con organismos y universidades internacionales conjuntamente con productores bananeros.

Anexo 3

Plan Estratégico de la ESPOL 2003 - 2007

PLAN ESTRATÉGICO ESPOL
2003-2007

PRESENTACIÓN

La formulación del Plan Estratégico de la ESPOL 2003-2007 responde a los siguientes principios:

- **Contextualizado**, para lo cual se consideró un conjunto de supuestos relacionados con la globalización, la sociedad del conocimiento, la competitividad, las tendencias de la ciencia y la tecnología, las características de la educación superior, la propuesta de un nuevo modelo de desarrollo regional con base en el conocimiento y el liderazgo que Guayaquil tiene como ciudad, hecho fundamental ahora que las ciudades también compiten y que como elemento de la globalización tiene relevancia y pertinencia el desarrollo de las capacidades locales.
- **La cabeza encabeza.** El proceso de formulación es liderado por la Alta Dirección Institucional. Igual responsabilidad tendrá en la ejecución y evaluación. La formulación del Plan tomó como referentes: (i) los planes de trabajo que el Rector y los Vicerrectores presentaron a consideración de la comunidad politécnica; y (ii) las resoluciones trascendentes del Consejo Politécnico referidas a asuntos institucionales de gran aliento.
- **Participativo y consensuado,** para lo cual, mediante varios mecanismos, se auscultó el criterio y expectativas de los tres estamentos politécnicos, considerando que es responsabilidad inexcusable de los profesores la dirección institucional; que los sujetos de la formac ión profesional son los estudiantes; y, que lo administrativo, en cuya cotidianidad están los trabajadores, es un soporte de la vida académica.
- **Mejoramiento continuo,** el Plan es solo una guía, es una obra perfectible y estará sujeto a cambios propios de la dinamia social y del vertiginoso crecimiento de la tecnología. Un elemento de este mejoramiento son las evaluaciones periódicas del plan y sus consecuentes reajustes.
- **Rendición de cuentas,** el plan, a más de fijar objetivos estratégicos y lineamientos para su cumplimiento, estableció indicadores de éxito para el período 2003-2004, de manera que una adecuada rendición de cuentas de directivos y de todos los estamentos deberá considerar esos indicadores, y bajo el principio de mejoramiento continuo fijarse indicadores para el período 2005-2007.

El proceso de formulación del Plan fue el siguiente:

a) **Elaboración del Borrador Cero por el Rectorado**, se tomó como referentes los logros institucionales hasta el 2002, los planes de trabajo presentados por las actuales autoridades, las resoluciones del Consejo Politécnico y los criterios de los miembros de este organismo en relación con el FODA Institucional.
b) **Análisis del Borrador Cero y procesamiento de las observaciones**, a través de medio electrónico, se envió el documento a la comunidad politécnica. El propósito fue que lo analicen y envíen al Rectorado las observaciones pertinentes hasta el 15 de julio, al e-mail: planesp@espol.edu.ec. Para fines de procesamiento se sugirió que cada observación especifique el asunto y la página correspondiente.
c) **Validación de los Borradores Uno y Dos**, mediante talleres del Consejo Politécnico Ampliado, en donde estuvieron representados todos los estamentos, organismos de apoyo, así como los ex rectores y ex vicerrectores. El propósito fue alcanzar un sólido consenso institucional que avale la decisión del Consejo Politécnico.
d) **Diálogo con los Estamentos,** en tres reuniones (10, 11 y 12 de noviembre), el Rector presentó ante los profesores, trabajadores y estudiantes, el Plan y recogió criterios que permitieron incluir, eliminar y reformular varios objetivos estratégicos.
e) **Aprobación del Plan por el Consejo Politécnico,** que es el acto formal y la ratificación del consenso alcanzado, hecho que ocurrió el 18 de noviembre del 2003.

El Plan consta de dos partes, la primera se integra de una presentación, una introducción y el análisis situacional; la segunda se refiere a los objetivos estratégicos que en un total de **55** se distribuyen en 7 capítulos así:

CAPITULO	OBJETIVO No.
Gestión Académica	1-13
Gestión Científica y Tecnológica	14-19
Gestión de las TICs	20-25
Vínculo con la comunidad	26-33
Bienestar Politécnico	34-43
Gestión Administrativo-Financiera	44-50
Desarrollo de la Infraestructura Física	51-55

Cada uno de estos capítulos se integra de un conjunto de objetivos estratégicos, identificando, para cada uno de ellos, tareas, lineamientos básicos, indicadores de éxito y fuentes de financiamiento.

Los objetivos estratégicos responden al análisis situacional, a los desafíos institucionales y a las políticas. Especial atención se le dio a aquellos que hacen relación con las cinco principales fortalezas, debilidades, oportunidades y amenazas identificadas por los líderes de la ESPOL.

Ejecutar con éxito el Plan Estratégico será la mejor prueba del compromiso que todos los estamentos, y en especial los directivos, tenemos con la principal fortaleza: el prestigio institucional.

En relación con el financiamiento, la mayoría de los objetivos académicos son autofinanciados, excepto el equipamiento de laboratorios, para lo cual se prevé dos grandes fuentes: Proyecto Ancón y Fundación ESPOL 50 años; los de Investigación, en su mayoría, se financiarán con el Proyecto VLIR-ESPOL; los de vínculos con la comunidad, en casi su totalidad, son autofinanciados y algunos generarán recursos para la ESPOL; en Bienestar Politécnico el principio fundamental es que "*el dinero de los estudiantes regresa a los estudiantes*", por ello los incrementos de los registros servirán para estos objetivos; los relacionados con gestión administrativa y financiera se financiarán con cargo al Presupuesto estatal y a las carreras y programas autofinanciados en la parte pertinente; en cuanto a la infraestructura física el financiamiento vendrá de recursos institucionales, Proyecto Ancón, Fundación ESPOL 50 Años (donaciones de Impuesto a la Renta).

Por su proceso participativo este Plan Estratégico es un esfuerzo colectivo de todos los estamentos bajo el liderazgo de la Alta Dirección.

Lo más complejo es ejecutarlo. Esa es la gran tarea y la principal responsabilidad de la Alta Dirección. Los estamentos son corresponsables y la rendición de cuentas es un mecanismo que les pertenece.

La mística de trabajo que caracteriza a los politécnicos nos acompañará a todos en este nuevo Desafío Institucional.

Moisés Tacle
RECTOR

INTRODUCCIÓN
Entre el pasado y el futuro

1. Lo que hemos hecho hasta ahora

La ESPOL surgió como respuesta a los requerimientos de profesionales técnicos en áreas fundamentales del desarrollo de la Costa. Desde sus inicios, su vida académica se articuló a las necesidades del sector productivo y se ejecutó bajo los principios de la excelencia. En estos primeros 45 años de vida, los grandes hitos institucionales son:

- **La creación a inicios de los años 60 de un espacio profesional para las ingenierías** en áreas como Petróleo, Minas, Marítima, Mecánica y Eléctrica, en el contexto de un aparato productivo de incipiente desarrollo industrial.
- **La formación de una planta de profesores** jóvenes, preparados en las mejores universidades del mundo, a quienes se les encargó la dirección institucional. A mediados de los años 70, la ESPOL tenía el cuerpo docente más joven del país y académicamente el más homogéneo. El 85% poseía título a nivel de maestría.
- **Un sistema de admisión** que, a través del examen de ingreso y el curso propedéutico, asegura que solo accedan a la ESPOL los bachilleres que posean los conocimientos y potencialidades para cursar con éxito los estudios politécnicos.
- **El Plan de Desarrollo 1983-1992**, cuya génesis arrancó a mediados de la década del 70, que significó la construcción del campus "Gustavo Galindo", la creación de las carreras de Acuicultura, Ingeniería en Computación, el Postgrado en Administración de Empresas y los Programas de Tecnología en Electricidad, Electrónica, Mecánica, Agrícola, del Mueble y la Madera; el mejoramiento de laboratorios y talleres; y, la capacitación docente.
- **Los Planes Estratégicos 1994-2002** que fueron las guías para incrementar los estudios de grado y postgrado (la ESPOL oferta 14 Programas de Tecnologías; 20 carreras de Tercer Nivel (Licenciaturas e Ingeniería) y 16 Programas de Postgrado); el involucramiento de la ESPOL en carreras económicas y con énfasis en los servicios como Economía, Ingeniería Comercial, Turismo, Ingeniería en Estadística en Informática, Auditoría y Control de Gestión; la decisión de que las nuevas carreras sean autofinanciadas; y, la creación y consolidación de varios mecanismos de vinculación con la empresa privada y la comunidad (Fundaciones, empresas, centros, series editoriales, etc.)
- **El Programa VLIR-ESPOL** a través del cual la Confederación de Universidades Flamencas (Bélgica) aportan recursos para cofinanciar un programa académico trascendente para la ESPOL, por su impacto en la Investigación, la creación del Centro de Tecnologías de la Información (CTI), del Centro de Investigaciones Biotecnológicas del Ecuador, CIBE, la

formación de recursos humanos a nivel de postgrado, en especial la Maestría Internacional en Acuicultura, la creación del Museo Interactivo de Ciencias. El VLIR-ESPOL se inició en 1998 y la segunda fase culminará en el 2008.

- ✔ **El Proyecto Ancón,** que se inició en 1996, y que a más de generar recursos a favor del Estado (regalías, cuando antes producía pérdidas por dos millones de dólares anuales) ha permitido mejorar la actividad petrolera en Ancón, proveer recursos que son trascendentes para la ESPOL, que se han invertido en el desarrollo institucional y asignar recursos para el desarrollo de la península de Santa Elena a través de: los planes estratégicos de los 4 cantones; becas del 100% y del 50% a favor de los bachilleres peninsulares; apoyo al turismo, agricultura, artesanía; mejoramiento de vías (Ancón-Santa Elena; Punta Carnero-Odebrecht, mediante la colaboración del MOP); y, el Programa de Mejoramiento de la Educación Primaria.
- ✔ **Hemos graduado a 8.032 profesionales** que por su alta formación científico-técnica, capacidad y valores éticos, el sector productivo, el sistema educativo y la sociedad los reconoce como actores claves del desarrollo nacional. Nuestros profesionales están insertados en el mundo laboral, hay gran demanda por ellos , han creado empresas y ocupan altos cargos de dirección en el sector público y privado.

2. Los nuevos desafíos

En la nueva sociedad donde el conocimiento, la información y las alianzas estratégicas son los ejes del desarrollo y la riqueza, la ESPOL tiene el gran desafío de modificar estructuras, procesos, medios y mecanismos para poder cumplir los fines inherentes a las universidades y escuelas politécnicas, ser el referente de la educación superior en el Ecuador y reconocida en el extranjero por su excelencia académica y por los resultados e impactos de los proyectos que ejecuta.

Elementos de ese gran desafío son:

Area Académica:

- ✔ Garantizar a los estudiantes, al sector productivo y al país que nuestras carreras de pregrado tienen el nivel científico y tecnológico requeridos que demanda la sociedad del conocimiento.
- ✔ Ofertar carreras que se adapten a los requerimientos de las demandas reales y potenciales del mercado y a las tendencias de la ciencia y la tecnología.
- ✔ Impartir una mejor educación y evaluarla de manera sistemática (una estrategia es pasar de una educación "centrada en el profesor" a una "centrada en el estudiante").
- ✔ Lograr que los profesores publiquen regularmente y participen con la comunidad los resultados de sus investigaciones y elucubraciones.

- ✔ Ofertar, con estándares internacionales, programas de postgrado en ciencia e ingeniería, el referente debe ser la Maestría en Acuicultura. Deben, en lo interno de la ESPOL, orientarse a consolidar la investigación, promover la innovación tecnológica, mejorar la calidad académica del pregrado, incrementar las actividades de extensión y publicación; y, deben, en lo externo, atender la demanda insatisfecha de postgrados en Ingeniería y Ciencias y fortalecer los nexos de la ESPOL con el sector empresarial.
- ✔ Ampliar y diversificar los programas de cooperación internacional, tomando como referente el VLIR-ESPOL.
- ✔ Asegurar una idónea transición generacional en la docencia.

Investigación

- ✔ Consolidar una política institucional sobre la formación y el trabajo cotidiano de los Ph.D y la investigación científico-tecnológica bajo el principio de Ciencia Util, esto es poner el conocimiento al servicio del desarrollo integral del Ecuador.

Vínculos con la comunidad/TICs

- ✔ Liderar el uso de las tecnologías de la información en la vida académica y su universalización en el sistema educativo nacional. Ese liderazgo debe hacer uso adecuado de las TICs para el procesamiento, almacenamiento y utilización de la información interna y externa como elemento clave de una gestión eficaz.
- ✔ Liderar la formulación y ejecución de grandes proyectos de vinculación con la sociedad, en especial los que hacen relación al desarrollo de las capacidades locales. Una estrategia hace relación a incorporar en la formación de nuestros estudiantes el tema de vinculación con la comunidad.
- ✔ Hacer realidad el Parque Tecnológico como expresión de un nuevo modelo de desarrollo regional con base en el conocimiento, la innovación y la creatividad, y como espacio para la gestión científica y tecnológica de la ESPOL y las universidades ecuatorianas.
- ✔ Fortalecer el liderazgo de la ESPOL en los temas trascendentes del país vinculados con nuestra vida académica.
- ✔ Consolidar los centros con énfasis en los vínculos con la comunidad y los CTDTs por nichos productivos y de servicios.
- ✔ Desarrollar programas relacionados al emprendimiento y a incubadoras de empresas de base tecnológica.
- ✔ Acreditar internacionalmente los laboratorios vinculados a la prestación de servicios.

Fortalecimiento Institucional

- ✔ Tener una estructura institucional ágil y flexible que se adapte a los cambios, sobre la base de las fortalezas y prestigio adquiridos.
- ✔ Cambiar paradigmas en relación con la estructura institucional, actualmente dividida en Facultades e Institutos.
- ✔ Consolidar y diversificar las fuentes de ingresos (Donación del Impuesto a la Renta, Canje de Deuda, Prestación de Servicios, Diversificación del campus Las Peñas, Formación de Empresas con Socios Estratégicos, otras alianzas estratégicas, etc.), para invertirlos en el desarrollo institucional y en programas que fortalezcan los vínculos con la comunidad.
- ✔ Conseguir, formular, presentar y ejecutar proyectos que generen recursos económicos que contribuyan de manera significativa a mejorar la gestión institucional.
- ✔ Llevar adelante el proceso de autoevaluación interna, externa y la acreditación institucional contemplados en la Ley de Educación Superior.
- ✔ Establecer un sistema de rendición de cuentas integral que evalúe la calidad de la educación, el cumplimiento del Plan Estratégico, entre otros aspectos (esta debería ser una tarea primordial de la Comisión de Evaluación Interna)
- ✔ Aprobar un nuevo Estatuto que modifique la estructura institucional.

ANÁLISIS SITUACIONAL

Por razones metodológicas el análisis situacional tiene 6 componentes:

1. El contexto mundial y nacional en el cual desarrolla su vida académica la ESPOL, así como el contexto interno expresado a través de los logros institucionales precedentes.
2. El análisis FODA
3. La Visión
4. La Misión
5. Valores
6. Políticas

1. El contexto mundial y nacional

1.1El contexto mundial

Las principales tendencias a nivel mundial en los próximos 5 años relacionadas con la educación superior son:

- ✔ Globalización de los mercados, nueva economía con base en el conocimiento.
- ✔ Mayor desarrollo de "nuevos materiales", electrónica, robótica y tecnologías de la información y la universalización de sus usos en la producción de bienes y servicios.
- ✔ Acelerado desarrollo de la biotecnología, los mayores cambios científico-tecnológicos se harán en el campo de la biología y biodiversidad.
- ✔ Los países del primer mundo, los "tigres asiáticos" y los que buscan mejorar su competitividad le otorgan merecida importancia a la innovación, la ciencia y la tecnología dentro de sus estrategias de desarrollo.
- ✔ Nuevas manifestaciones de la competitividad. No solo competirán los organismos empresariales, también lo harán las ciudades, lo cual exigirá mayor calidad de las capacidades locales.
- ✔ Acelerado desarrollo de sistemas "Multimedios" y de la " Universidad Virtual".
- ✔ Mayor demanda de educación terciaria y de postgrado. Las universidades de los países desarrollados centran su mayor esfuerzo académico en los programas de postgrado por sobre los estudios de grado.
- ✔ Las universidades de prestigio fortalecerán sus fondos patrimoniales y sus mecanismos de autogeneración de rentas.
- ✔ Se fortalecerán las relaciones de cooperación entre universidades y escuelas politécnicas de prestigio, a nivel latinoamericano.
- ✔ Ganará adhesión la tesis de que "las universidades detentan la clave de la economía y de la sociedad del conocimiento"[1].

[1] El Papel de las Universidades en la Europa del Conocimiento

- ✔ Organismos multilaterales como el BID, Banco Mundial, CAF financiarán iniciativas relacionadas con el emprendimiento, uso de las TICs en la educación y el desarrollo de las capacidades locales.
- ✔ Cambios radicales en las modalidades de contratación de profesionales: disminuirá el porcentaje a dependencia; crecerá el autoempleo, la contratación de mujeres; el trabajo en casa.
- ✔ Nuevos actores que no son universidades incrementarán la oferta de capacitación, en especial para la Alta Dirección.
- ✔ La Educación Continua y la capacitación permanente crecerán, tres factores serán fundamentales: los procesos demográficos, la vida útil de los trabajadores y el desarrollo de las TICs.
- ✔ La migración de profesionales de tercer y cuarto nivel desde los países pobres y emergentes hasta los países desarrollados, con lo cual países como el Ecuador pierden su más valioso recurso: el capital humano.
- ✔ Una mayor preocupación por alcanzar los objetivos del desarrollo sostenible, por generar tecnologías limpias amigables con la naturaleza, incorporar procesos participativos en el manejo de los recursos naturales y en fortalecer la cooperación entre los países.
- ✔ Mayor adhesión y aplicación de los aprendizajes fundamentales propuestos por UNESCO: aprender a conocer (conocimiento a profundidad); aprender a hacer (relación teoría y práctica y alta participación); aprender a vivir juntos (práctica de la democracia, la tolerancia, el respeto a los demás; aprender a ser (autoestima, liderazgo, innovación).
- ✔ Cada vez más mujeres obtienen grados académicos y ocupan cargos de dirección en el sector privado y público.
- ✔ Gran movilidad de los recursos humanos altamente calificados; en consecuencia, las universidades deben formar profesionales emprendedores con estándares internacionales para que sean competitivos y las universidades de los países en desarrollo tendrán la oportunidad de captar a precios bajos "masa crítica" de jubilados de los países ricos, y científicos de los ex países socialistas.
- ✔ Diferenciación de las redes universitarias por la calidad de sus miembros. Tendrán reconocimiento las redes integradas por universidades de prestigio.
- ✔ Mayor preocupación por las energías alternativas, en especial el uso del hidrógeno.
- ✔ Crecimiento del sector terciario de la economía.
- ✔ Consolidación de las PYMES por la calidad de sus emprendedores, el uso de tecnologías y los altos índices de competitividad.

1.2 El contexto nacional

A más del impacto de las tendencias mundiales, las principales tendencias a nivel nacional en los próximos 5 años que incidirán en el quehacer de las universidades y escuelas politécnicas son:

- ✔ Mayor preocupación de las familias por dar a sus hijos educación de calidad.
- ✔ Fortalecimiento del bachillerato polivalente.
- ✔ Crecimiento de la demanda por educación superior, en especial de las tecnologías de la información, tercer nivel (ingenierías, licenciatura) y postgrado.
- ✔ Uso de las empresas de los fondos que maneja el Consejo Nacional de Capacitación y Formación Profesional (CNCF), pues requerirán capacitar a sus recursos humanos para mejorar la productividad.
- ✔ Preocupación de las municipalidades por liderar los desarrollos locales, tomando como referencia las gestiones exitosas de grandes, medianas y pequeñas ciudades, lo cual requerirá respuestas de las universidades y escuelas politécnicas (*Rol de las Universidades en el Desarrollo Regional y Local*).
- ✔ Cada vez más mujeres tienen grados académicos y se insertan al mercado laboral.
- ✔ Esfuerzos compartidos entre el Estado, las empresas y las universidades a favor de la competitividad.
- ✔ Desarrollo de la mediana, pequeña y micro empresas como opción para generar empleo masivo y enfrentar la pobreza y la migración. Parte de este desarrollo se financiará con las "remesas" de los migrantes.
- ✔ Surgimiento de empresas de base tecnológica. Se reactivarán las ideas de las incubadoras de empresas y de los parques tecnológicos.
- ✔ Mayor peso demográfico de la cuenca baja del Guayas, en especial de la Península de Santa Elena.
- ✔ Mayor crecimiento del sector terciario de la economía.
- ✔ Mayor presencia de universidades extranjeras.
- ✔ Las rentas estatales a favor de los centros de régimen público se mantendrán sin cambios significativos.
- ✔ Guayaquil se consolidará como ciudad competitiva (mayor inversión privada nacional y extranjera, liderazgo del Municipio).

1.3 El contexto interno

En el período 1997-2002 los grandes logros institucionales fueron:

- ✔ Se continuó con los procesos académicos exitosos.
- ✔ Se fortalecieron los programas de postgrado en las unidades académicas.
- ✔ Se fortaleció la investigación científica.
- ✔ Se avanzó en el posicionamiento de la ESPOL a nivel internacional.
- ✔ Se obtuvo y ejecutó el proyecto VLIR-ESPOL.

- ✔ Se incorporó a doctores (PhD) y magíster a la planta docente de la ESPOL.
- ✔ Se lideró el uso de las nuevas tecnologías de la información en el campo educativo, en especial en la Península de Santa Elena (red de 20 escuelas) y mediante el Programa Maestr@com.
- ✔ Se potenció el área agropecuaria.
- ✔ Se incrementó la cobertura geográfica de la oferta educativa.
- ✔ Se mejoró el sistema de admisión y se incrementó la infraestructura académica, deportiva y de servicios a estudiantes.
- ✔ Se promovió la constitución de fondos.
- ✔ Se incrementaron de manera sustancial las becas y los créditos educativos.
- ✔ Se manejó de manera adecuada, al interior de la ESPOL, la crisis económica del país.
- ✔ Se formuló una propuesta de desarrollo regional con base en el conocimiento.
- ✔ Se incrementó la experiencia de la ESPOL en el tema social y en el trabajo comunitario, en especial en la Península de Santa Elena.
- ✔ Se fortalecieron los vínculos de la ESPOL con los sectores productivos privado y público.
- ✔ Se incrementó el prestigio ético de la ESPOL en la comunidad nacional.
- ✔ Se defendió la integridad del campus Gustavo Galindo.
- ✔ Se otorgó el Doctorado Honoris Causa a personalidades.
- ✔ Se posicionó como referente en las investigaciones del Fenómeno de El Niño.

2. Análisis FODA

Las cinco principales fortalezas de la ESPOL son:

No.	Fortaleza	Impacto
1	La imagen de la ESPOL en Guayaquil, en la sociedad ecuatoriana y en el exterior.	8.8
2	La calidad de la enseñanza teórica impartida.	6.13
3	La experiencia actual del personal docente.	5.79
4	La planificación estratégica.	5.71
5	La calidad de los servicios educativos politécnicos.	5.63

Las 5 principales debilidades son:

No.	Debilidades	Impacto
1	La ausencia de un sistema de medición integral de desempeño en la gestión administrativa.	7.07
2	La ausencia de instrumentos de medición integrales del desempeño de los profesores.	6.32
3	La dependencia de la ESPOL de los fondos estatales.	5.6
4	El empleo que se le da a los resultados de las encuestas del CISE.	5.24
5	El sistema vigente de la ESPOL para controlar la calidad de enseñanza impartida.	4.45

Las 5 principales oportunidades son:

No.	Oportunidades	Impacto
1	Los programas de becas y de capacitación en el exterior.	8.22
2	La aceptación de nuestros profesionales en el medio	7.89
3	La captación de un porcentaje del impuesto a la renta	7.80
4	Inicio de la sociedad del conocimiento en el concierto mundial	7.53
5	El avance omnipresente de la tecnología	7.37

Las 5 principales amenazas son:

No.	Amenazas	Impacto
1	El posible fracaso de la dolarización	7.68
2	La inestabilidad política del país	7.59
3	La eventual reducción del Presupuesto estatal	7.13
4	El nivel de desempleo y subempleo.	6.34
5	La deuda externa	6.26

3. Visión Institucional

Ser líder y referente de la Educación Superior de América Latina.

4. Misión Institucional

Formar profesionales de excelencia, líderes, emprendedores, con sólidos valores morales y éticos que contribuyan al desarrollo del país, para mejorarlo en lo social, económico, ambiental y político. Hacer investigación, transferencia de tecnología y extensión de calidad para servir a la sociedad.

5. Valores

Los valores que más se practican en la ESPOL son:

- **Compromiso con la excelencia académica**: La excelencia académica es una meta superior, permanente y cotidiana. Es la condición básica para que las universidades y escuelas politécnicas cumplan la finalidad que la Constitución y Ley determina.

- **Mística de Trabajo**: Trabajar y cumplir para que la ESPOL amplíe su prestigio.

- **Responsabilidad**: Cumplir con calidad y a tiempo todas las tareas institucionales. Cumplir todos y asumir las consecuencias de las acciones y omisiones.

- **Honestidad**: Manejar los asuntos personales e institucionales con integridad y probidad.

- **Imparcialidad:** Independencia en las decisiones institucionales. Las relaciones con nuestros aliados estratégicos son entre pares y de cooperación recíproca, y tienen como finalidad la búsqueda de la verdad y el desarrollo integral del Ecuador.

6. **Políticas Institucionales**

- Trabajar con estándares internacionales para garantizar la excelencia académica.
- Ampliar los vínculos de colaboración a nivel mundial con instituciones de excelencia para fortalecer nuestras actividades académicas.
- Fortalecer los vínculos con los actores claves del Ecuador para asegurar la pertinencia del quehacer politécnico.
- Poner el adelanto tecnológico y la cultura emprendedora al servicio del desarrollo humano.
- Orientar las inversiones a favor de la excelencia académica y el bienestar politécnico.
- Promover el cultivo y práctica de los valores éticos y morales.

PLAN ESTRATÉGICO DE LA ESPOL 2003-2007

Parte Segunda: Objetivos Estratégicos

- Gestión Académica
- Gestión Científica y Tecnológica
- Gestión de las TICs
- Vínculo con la comunidad
- Bienestar Politécnico
- Gestión Administrativo-Financiera
- Desarrollo de la Infraestructura Física

CAPITULO I
GESTION ACADEMICA

El éxito o el fracaso de las personas y las naciones, así como la prosperidad de la humanidad, dependen de que podamos desarrollar apropiadamente nuestros recursos humanos. En este siglo varios elementos intangibles como la información y la creatividad, darán a los países ventajas competitivas.

Kim Dae-Jung
Presidente de la República de Corea

Las destrezas adquiridas mediante la educación secundaria y terciaria permiten que las empresas **adopten y adapten** las tecnologías existentes de manera más eficiente y que capaciten a sus trabajadores. Las destrezas adquiridas en el nivel de postgrado (en especial, pero no exclusivamente, en áreas como la ciencia y la ingeniería) permiten que las empresas **creen y desarrollen** nuevas tecnologías.

"Cerrando la Brecha en Educación y Tecnologías", Banco Mundial, 2003

OBJETIVOS

1. Reestructurar el sistema de admisión de las carreras de pregrado.
2. Ofertar programas específicos de inserción de los tecnólogos a las carreras de Ingeniería.
3. Ofertar programas de Licenciatura para los Tecnólogos.
4. Crear las Licenciaturas en Ciencias con mención en Educación.
5. Incrementar la oferta de Ingenierías con la actual estructura.
6. Ofertar asignaturas, carreras y programas mediante modalidad a distancia.
7. Consolidar el programa de becas en el extranjero para formar recursos humanos al más alto nivel académico.
8. Completar y modernizar la infraestructura técnica del Centro de Información Bibliotecaria, Laboratorios y Talleres.
9. Incluir en las Ingenierías la mención en Biotecnología.
10. Crear las políticas y estructuras curriculares de la era del conocimiento, para fortalecer nuestra vida académica.
11. Diseñar y ejecutar el Plan de Perfeccionamiento Docente.
12. Incrementar la oferta de programas de Postgrado en Ciencias e Ingenierías.
13. Medir, de manera objetiva, sistemática y permanente la calidad de la educación que impartimos.

Objetivo 1
Mejorar el sistema de admisión de las carreras de pregrado de la ESPOL

Desafío/Tarea

El Vicerrector General presentará el proyecto correspondiente a la Comisión Académica para ejecutarlo desde el año 2004.

Lineamientos

- ✔ Establecer un proyecto de perfeccionamiento para los docentes de las instituciones de educación media.
- ✔ Ofertar el servicio de acreditación a los colegios del país.
- ✔ Ejecutar un Plan promocional de la ESPOL hacia la comunidad.
- ✔ Analizar la pertinencia de que haya requerimientos distintos para el ingreso a las diferentes carreras de pregrado.
- ✔ Establecer un Programa de Formación para profesores y ayudantes académicos del prepolitécnico.
- ✔ Fomentar un ciclo de charlas de orientación profesional a los estudiantes del curso prepolitécnico.

Indicadores de Éxito

2003: La Comisión Académica aprobó el Plan presentado por el Vicerrector General.
2004: Se iniciaron los Planes de Perfeccionamiento Docente y de Promoción.
Se incrementó el número de estudiantes y el porcentaje de aprobación del curso prepolitécnico fue superior a 40.

Fuente de Financiamiento

Presupuesto ESPOL y autofinanciamiento.

Objetivo 2
Ofertar programas específicos de inserción de los Tecnólogos a las carreras de Ingeniería

Desafío/Tarea

El Vicerrector General presentará un proyecto a la Comisión Académica en el año 2003.

Lineamientos

- ✔ Cada Programa de Inserción estará acorde con la carrera de Ingeniería seleccionada por el aspirante.
- ✔ Los Programas de Inserción deben ser autofinanciados.
- ✔ Los programas de inserción pueden ser aprobados vía examen.
- ✔ Establecer una promoción efectiva de este programa.

Indicadores de Éxito

2004: El Consejo Politécnico aprobó los Programas de Inserción correspondiente y se iniciaron los Programas.

Fuente de Financiamiento

Autofinanciada.

Objetivo 3
Ofertar Programas de Licenciatura para los Tecnólogos

Desafío/Tarea

- ✔ El Instituto de Tecnologías presentará ante el Consejo Politécnico, en el 2003, la propuesta de creación de varias Licenciaturas: Gestión de las Tecnologías y Diseño Gráfico. También auscultará la pertinencia de la licenciatura en Procesos de la Alta Dirección.
- ✔ La FIEC y el PROTCOM ofertarán en el 2003 la Licenciatura en Multimedia que aprobó el Consejo Politécnico en el 2002.

Lineamientos

- ✔ Los programas de licenciatura estarán acordes a lo establecido por el CONESUP.
- ✔ Los Programas de Licenciatura serán dictados por el Instituto de Tecnologías o en forma conjunta con otra unidad de la ESPOL.
- ✔ La propuesta de creación incluirá un estudio de mercado mostrando la pertinencia de las carreras y la demanda real y potencial.
- ✔ Estos programas serán autofinanciados.

Indicadores de Éxito

2004: El Consejo Politécnico aprobó por lo menos un Programa de Licenciatura para los Tecnólogos.
Los Programas de Licenciatura están en ejecución.

Fuente de Financiamiento

Autofinanciada.

Objetivo 4
Crear las Licenciaturas en Ciencias con mención en Educación

Desafío/Tarea

Una Comisión constituida por delegados de los correspondientes Institutos y del Vicerrectorado General presentará en el 2003 la o las propuestas de creación.

Lineamientos

- ✔ Será un proyecto piloto o experimental.
- ✔ Tendrá 5 semestres de duración, pues, para acceder se requiere haber aprobado el Ciclo Básico de la ESPOL o tener título de ingeniero.
- ✔ En cada semestre se trabajarán 3 áreas interrelacionadas: a) Especialización; b) Educación; c) Tecnologías y Humanísticas.
- ✔ Las áreas de Educación y la de Tecnologías y Humanísticas serán comunes para todos los licenciaturas.
- ✔ Cada Instituto designará una Comisión de Convalidación de materias.
- ✔ Deberá utilizar las TIC's, desarrollar habilidades en Gestión Educativa, Informática, Comunicación y Expresión, y dominio de un idioma extranjero.
- ✔ Utilizará como base las materias de Ciencias dictadas por los Institutos.

Indicadores de Éxito

2004: El Consejo Politécnico aprobó el proyecto presentado por la Comisión y se inició el Programa.

Fuente de Financiamiento

Presupuesto del Estado y autofinanciadas en los recursos extras que requiera la ESPOL (considerar becas).

Objetivo 5
Incrementar la oferta de Ingenierías, con la actual estructura

Desafío/Tarea

Cada unidad académica presentará en el año 2004, sola o asociada con otra u otras unidades de la ESPOL, por lo menos, una nueva carrera de Ingeniería, siguiendo los lineamientos básicos siguientes:

Lineamientos Básicos

- ✔ Estar articulada a los requerimientos y tendencias del aparato productivo nacional y regional.
- ✔ Poseer estándares académicos internacionales.
- ✔ Ofertar el 100% de los créditos con profesores de cuarto nivel.
- ✔ Tener un currículo muy flexible que permita aprovechar las mallas curriculares existentes (formar profesionales interdisciplinarios/"ingenierías híbridas").

Indicadores de Éxito

2004: El Consejo Politécnico aprobó dos nuevas carreras de Ingeniería sobre la base existente, ante la Comisión Académica.
2005: Inicio de las nuevas carreras.

Fuente de Financiamiento

Autofinanciada y Presupuesto del Estado.

Objetivo 6
Ofertar asignaturas, carreras y programas mediante modalidad a distancia

Tarea/Meta

El Rectorado presentará el Plan de Educación a Distancia de acuerdo con los siguientes lineamientos:

Lineamientos

- ✔ Toda la oferta debe hacerse con estándares académicos internacionales.
- ✔ Se considerará la experiencia adquirida en los cursos prepolitécnicos "virtuales".
- ✔ Previo a la oferta, la ESPOL deberá haber formado su masa crítica en modalidad a distancia.
- ✔ Los contenidos programáticos son responsabilidad de las unidades académicas; los aspectos tecnológicos del CTI; y, los operativos serán definidos por el Rectorado.
- ✔ La oferta de una carrera mediante la modalidad a distancia requerirá de la aprobación del Consejo Politécnico.
- ✔ Estos programas serán autofinanciados.

Indicadores de Éxito

2004: El Consejo Politécnico aprobó el Plan de Educación a distancia.

Fuente de Financiamiento

Autofinanciada.

Objetivo 7

Consolidar el Programa de Becas en el extranjero para formar recursos humanos al más alto nivel académico

Desafío/Tarea

La Comisión Académica, con el apoyo de la Oficina de Relaciones Externas en el aspecto operativo, presentará ante el Consejo Politécnico el plan correspondiente.

Lineamientos

- ✔ Con recursos institucionales, incluidas las carreras autogestionarias, se privilegiará la formación de Ph.D en áreas definidas por consenso, concordante con los proyectos de investigación institucional. Se aprovechará el Programa Albán para formar en Europa los profesionales de cuarto nivel que la ESPOL requiere para potenciar sus programas académicos y para concretar el relevo generacional.
- ✔ Se aprovechará el Proyecto VLIR-ESPOL y los diferentes mecanismos de cooperación internacional (La ESPOL tiene más de 60 convenios con universidades de prestigio) para formar profesionales de cuarto nivel, poniendo énfasis en la formación de Ph.D.
- ✔ Se utilizará la modalidad compartida para formar Ph.D en la ESPOL.
- ✔ Las becas para hacer estudios de pregrado en el extranjero serán aprobadas por el Consejo Politécnico.
- ✔ Los Ph.D que forme la ESPOL y los que logre captar deben ser aprovechados, en especial en los postgrados, en proyectos de investigación y en los proyectos de vínculos con la comunidad, en especial los que hacen relación al uso de tecnologías.

Indicadores de Éxito

2003: El Consejo Politécnico aprobó el Plan y se envían al extranjero por lo menos 20 nuevos becarios.

Fuentes de Financiamiento

Ancón, autofinanciado, cooperación internacional, Programa Albán.

Objetivo 8

Completar y modernizar la infraestructura técnica del Centro de Información Bibliotecaria, Laboratorios y Talleres

Desafíos/Tareas

El Vicerrector General conformará y presidirá una Comisión encargada de establecer los requerimientos de cada unidad académica en concordancia con los objetivos académicos del Plan Estratégico.

Lineamientos Básicos

- ✔ Modernizar y actualizar el Centro de Información Bibliotecaria y los Laboratorios acorde con las exigencias de la sociedad del conocimiento.
- ✔ Universalizar el uso de las tecnologías de la información en las actividades académicas, de investigación y de servicios para mejorar la capacidad institucional en la generación de conocimientos y la formación y capacitación de los "trabajadores del conocimiento".
- ✔ Incorporar las tecnologías de punta que requiera la formación de estudios de grado y postgrado que oferta y ofertará la ESPOL.
- ✔ Manejar y usar con visión institucional los laboratorios que poseen las unidades académicas y centros, para optimar su inversión, evitar la duplicación de recursos.
- ✔ Promover que los CTDTs que resuelva crear el Consejo Politécnico adquieran laboratorios y equipos mediante donaciones.
- ✔ Establecer alianzas estratégicas con entidades públicas y privadas que posean laboratorios de última tecnología, con el objeto de que los estudiantes politécnicos accedan a dichos laboratorios.
- ✔ Destinar un porcentaje de la renta anual del Proyecto Ancón durante 5 años, para completar y modernizar los laboratorios y talleres. Este porcentaje lo definirá el Consejo Politécnico.
- ✔ La inversión en laboratorios se hará de acuerdo con las prioridades institucionales.

Indicadores de Exito

2004: La Comisión hizo el inventario de necesidades.
El Consejo Politécnico definió el porcentaje de los recursos del Proyecto Ancón para cumplir con este objetivo.

Fuente de Financiamiento

Proyecto Ancón, Autofinanciado: donaciones, alianzas estratégicas, Prepolitécnico, Registros en especial para las aulas.

Objetivo 9
Incluir en las Ingenierías la mención en Biotecnología

Desafío/Tarea

La Comisión Académica presentará en el 2004, con el apoyo del CIBE, la propuesta para formar ingenieros con mención en Biotecnología.

Lineamientos Básicos

- ✔ Integrarla al Plan de Biotecnología de la ESPOL.
- ✔ Incluir Biología como materia obligatoria en el prepolitécnico para las ingenierías de origen Químico-Biológico.
- ✔ Incluir Biología como materia obligatoria del Ciclo Básico.
- ✔ Fortalecer en las ingenierías el área de Biotecnología.
- ✔ Incorporar PhD y Magister especializados en Biología y Biotecnología a la planta de profesores e investigadores de la ESPOL, en especial los formados en el VLIR-ESPOL..
- ✔ Ser autofinanciada.

Indicadores de Éxito

2004: El Consejo Politécnico aprobó la propuesta por el Consejo Politécnico y se inició el Programa.

Fuente de Financiamiento

Autofinanciada.

Objetivo 10

Crear las políticas y estructuras curriculares de la era del conocimiento para fortalecer nuestra vida académica

Tarea/Desafío

Bajo la dirección del Rector se creará un equipo interdisciplinario que presentará al Consejo Politécnico el proyecto respectivo.

Lineamientos

- ✔ La economía y la sociedad del conocimiento nacen de la combinación de cuatro elementos interdependientes: la producción del conocimiento, esencialmente por medio de la investigación científica, su transmisión mediante la educación y la formación, su difusión a través de las tecnologías de la información y la comunicación, y su explotación a través de la innovación tecnológica.
- ✔ La nuevas tecnologías de la información y la comunicación aceleran la tendencia de la internacionalización de la educación superior a nivel profesional y a nivel de postgrado.
- ✔ Los procesos demográficos y la economía del conocimiento contribuyen a incrementar la oferta de Educación Continua, en especial la relativa a la actualización profesional y la incorporación de nuevas habilidades y destrezas laborales.
- ✔ La ESPOL debe aprovechar las oportunidades para buscar y obtener recursos internacionales no reembolsables que financien proyectos que fortalezcan la vida académica y aporten al desarrollo del país.
- ✔ La ESPOL posee una importante infraestructura tecnológica, convenios internacionales y recursos humanos calificados para llevar adelante tareas de esta naturaleza.

Indicadores de Éxito

2003: El Rector designó la Comisión.
2004: Primer semestre: El Consejo Politécnico conoció la propuesta de la Comisión designada por el Rector.

Fuente de Financiamiento

Presupuesto ESPOL.

Objetivo 11
Diseñar y Ejecutar el Plan de Perfeccionamiento Docente

Desafío/Tarea

El CISE, el CTI y la Comisión Académica, presentarán ante el Consejo Politécnico, en el año 2003, el Plan de Perfeccionamiento Docente de la ESPOL.

Lineamientos Básicos

- ✔ El Plan incluirá la oferta de un Programa Doctoral y Maestrías mediante Diplomados Acreditables.
- ✔ Los módulos y/o diplomados podrían ser (i) Rol de las Universidades y Escuelas Politécnicas en el Siglo XXI; (ii) Andragogía; (iii) Gestión del aprendizaje; (iv) Gestión en centros de educación superior; (v) Incorporación de las TICs en el aula; (vi) Metodologías Específicas (proyectos, marco lógico, casos, dirección de tesis, por ejemplo); (vii) Habilidades de facilitación; (viii) Investigación educativa; (ix) Gerenciamiento del Conocimiento, (x) Mapas Conceptuales, (xi) Diseño Instruccional, (xii) Aprendizaje basados en problemas, (xiii) Psicología Educativa, (xiv) Consejería, asesorías y tutorías académicas y/o profesionales; (xv) Negociación, entre otros.
- ✔ Uno o más módulos y/o diplomados, total o parcialmente, serán "virtuales".
- ✔ Los profesores que cumplan con los requisitos legales de graduación obtendrán el título de Master y/o Doctor en Educación Superior, según el caso.
- ✔ La ESPOL financiará a sus profesores el 80% del valor de la colegiatura, con cargo al Fondo de Docencia.
- ✔ La Maestría poseerá estándares internacionales y por lo menos el 50% de los créditos serán dirigidos por profesores que tengan título de Ph.D y reconocida solvencia académica.
- ✔ El programa de Maestría debe ser continuo y sistemático; considerar las modalidades presencial, semipresencial y virtual; los horarios serán planificados en coordinación con las unidades académicas para facilitar la participación de docentes y ayudantes académicos.
- ✔ El Plan también considerará las políticas institucionales relacionadas con el año sabático.

Indicadores de Éxito

2004: El Consejo Politécnico aprobó el Plan de Perfeccionamiento, y el CONESUP la Maestría en Educación Superior.

2004: El 10% de los profesores con nombramiento inició la Maestría en Educación Superior.
Mejoró el promedio de evaluación docente de los profesores que inician la primera promoción de la Maestría.

Fuente de Financiamiento

Proyecto Ancón, Presupuesto ESPOL; Autofinanciamiento.

Objetivo 12
Incrementar la oferta de Programas de Postgrado en Ciencias e Ingenierías

Desafío/Tarea

Cada unidad académica presentará en el año 2003, sola o asociada con otra unidad de la ESPOL u otra universidad o escuela politécnica del extranjero o un consorcio de universidades del Ecuador, por lo menos, un Programa de Postgrado, siguiendo los lineamientos básicos siguientes:

Lineamientos Básicos

- ✔ Poseer estándares académicos internacionales.
- ✔ Estar articulados a proyectos de investigación.
- ✔ Responder a los requerimientos y tendencias del aparato productivo nacional, en el contexto de la competitividad mundial.
- ✔ Satisfacer la demanda de la ESPOL y de otras instituciones de educación superior.
- ✔ Ser autofinanciado.
- ✔ Ofertar, por lo menos, el 35% de los créditos con profesores que tienen título de PhD.
- ✔ La Maestría podría tener un núcleo común de cursos; un área de transición y una o dos especializaciones según las fortalezas existentes en la institución o en el consorcio de universidades.
- ✔ Otorgar becas a profesores de la ESPOL (Fondo de Docencia).
- ✔ Permitir que estudiantes del último término del pregrado tomen créditos.

Indicadores de Éxito

2003: El CONESUP aprobó, por lo menos, cuatro programas de postgrado en Ciencias e Ingeniería presentados por la ESPOL, uno de ellos el de Biotecnología con el apoyo económico del sector bananero (FBI).

2004: Se inició por lo menos 2 programas y se presentan al CONESUP otros 3 programas.

Fuente de Financiamiento

Autofinanciada y Proyecto Ancón.

Objetivo 13
Medir, de manera objetiva, sistemática y permanente, la calidad de la educación que impartimos en la ESPOL

Desafío/ Tarea

Diseñar y desarrollar instrumentos para medir la calidad de la educación que impartimos en el ICM y en otras unidades de la ESPOL.

Lineamientos Básicos

- ✔ Compendiar las variables que conviene medir.
- ✔ Diseñar los indicadores de calidad y la manera de medirlos.
- ✔ Formular el plan de medición.
- ✔ Obtener resultados y procesarlos para una primera publicación.

Indicadores de Éxito

2004 Primer semestre: En nueve meses, a partir de la aprobación de Plan, el ICM publicó los primeros resultados de la gestión de medición de la calidad (Pregrado, Postgrado e Investigación).

Fuente de Financiamiento

Presupuesto ESPOL.

CAPITULO II
GESTION CIENTÍFICA Y TECNOLOGICA

> **"El crecimiento de la sociedad del conocimiento depende de la producción de nuevos conocimientos, su transmisión, a través de la educación y la formación, su divulgación a través de las tecnologías de la información y la comunicación y su empleo por medio de nuevos procedimientos industriales de servicio. Las universidades son únicas en este sentido, ya que participan en todos estos procesos..."**
> "*Comisión Europea: El papel de las universidades en la Europa del Conocimiento*". **05.02.2003**

Objetivos

14. Establecer estrategias y políticas para el fortalecimiento de la investigación científica y tecnológica de la ESPOL .
15. Proporcionar, desarrollar y fortalecer las capacidades de investigación y su gestión en la ESPOL.
16. Publicar los avances y resultados de los proyectos de investigación en los órganos de difusión internos y en revistas indexadas.
17. Publicar libros relevantes para la educación superior y otros ligados a la investigación y desarrollo en la ESPOL.
18. Impulsar y desarrollar la creatividad para proyectos de innovación tecnológica.
19. Promover y financiar investigaciones que generen invenciones susceptibles de ser explotadas, y crear las condiciones institucionales para generar ingresos provenientes de patentes, marcas registradas y otras formas previstas en las leyes ecuatorianas.

Objetivo 14
Establecer estrategias y políticas para el fortalecimiento de la Investigación Científica y Tecnológica en la ESPOL

Desafío/Tarea

Definir los elementos de políticas y estrategias de desarrollo científico-tecnológico introduciendo la Visión. Este Plan deberá ser integrador de la comunidad politécnica, vinculante con el sector externo, flexible y adaptable a las necesidades cambiantes y los requerimientos presentes y futuros, tendrá como uno de sus referentes el Proyecto VLIR/ESPOL.

Lineamientos

- ✓ Integrar elementos de prospectiva tecnológica para la fijación de áreas prioritarias y desarrollo futuro científico-tecnológico de la institución.
- ✓ Afianzar vínculos con sectores externos, comunitarios y productivos de desarrollo nacional e internacional.
- ✓ Consolidar y difundir el acervo científico de la ESPOL.
- ✓ Captación institucional del conocimiento externo valedero científico-tecnológico.
- ✓ Reformar los estatutos y reglamentos para establecer estímulos que fomenten el interés por trabajar en ciencia y aplicación de tecnología.
- ✓ Establecer mecanismos de financiamiento para Ciencia y Tecnología.
- ✓ Articular un sistema adecuado para la interacción real entre investigadores y sector productivo.
- ✓ Establecer las políticas para trabajar en Investigación Básica, Aplicada y Transferencia tecnológica.
- ✓ El CICYT administrará el 6% del presupuesto de la ESPOL para el desarrollo de la investigación y velará por su vinculación con las actividades culturales, publicaciones y postgrados.
- ✓ El CICYT contará con nuevas instalaciones físicas que proporcionará un ambiente propicio para el desarrollo de la investigación.

Indicadores de Exito

2003: Entrega del Plan Estratégico de la gestión en Ciencia y Tecnología (incluirá las áreas prioritarias).
Entrega de propuesta de la reforma del Estatuto y reglamentos de Investigación.
El CICYT presentará los planos y conseguirá la aprobación del acondicionamiento físico.
El Consejo de Investigación presentará al Consejo Politécnico una propuesta para definir las áreas prioritarias.

2004: Se creó un Comité Asesor para la investigación, integrado por representantes del sector productivo.
La ESPOL asignó el 6% del presupuesto para la investigación y se ejecutó de acuerdo con el Plan Estratégico del CICYT-ESPOL.
Culminó la ampliación del CICYT.

Fuente de Financiamiento

Proyecto VLIR-ESPOL..

Objetivo 15
Proporcionar, desarrollar y fortalecer las capacidades de investigación y su gestión en la ESPOL

Desafío / Tarea

El CICYT gestionará y apoyará la consecución de fondos para la ejecución de proyectos de investigación en toda la ESPOL y preparará la apertura de un fondo especial para proyectos tipo semillas.

Lineamientos Básicos

- ✓ Establecer, fomentar la comunicación y participación entre el CICYT, las Unidades Académicas y los Centros de la ESPOL vinculados a la Ciencia y Tecnología.
- ✓ Realizar actividades de capacitación en formulación, implementación y evaluación de proyectos de investigación.
- ✓ Capacitar al personal del CICYT en tareas de coordinación de proyectos.
- ✓ Fortalecer las capacidades de gestión para la investigación en la ESPOL, incluyendo la búsqueda y captación (negociación) de recursos internacionales, la coordinación de proyectos, su evaluación y replicabilidad.
- ✓ Definir en la carga politécnica del profesor de la ESPOL, el tiempo de dedicación exclusiva para la Investigación, en concordancia entre la Unidad Académica y el CICYT.
- ✓ Preparar conjuntamente (CICYT y Unidad Académica) el Plan de Año Sabático para profesores que realicen actividades de investigación como actividad prioritaria en ese periodo.
- ✓ Establecer una estrategia institucional para la formación de Ph.D con una proyección especial en las líneas prioritarias de investigación.
- ✓ Proporcionar y difundir síntesis de las actividades de investigación que se realizan en la ESPOL para establecer grupos afines complementarios y evitar la duplicación de esfuerzos.
- ✓ Regular y canalizar todas las investigaciones y actividades ligadas con la misma en la ESPOL.
- ✓ El CICYT contará con asistencia financiera para el manejo de Proyectos de Ayuda Externa.
- ✓ El CICYT contará con una estructura profesional moderna que le permita buscar fondos, formular y ejecutar proyectos.
- ✓ Se explorará la posibilidad de firmar contratos de gestión para obtener recursos no reembolsables.

Indicadores de Éxito

2003: Se presentó la propuesta conjunta con las Unidades Académicas para establecer estrategia de formación de Ph.D., tiempo de investigación e investigaciones en sabático y pasantías.

Se realizaron 2 eventos para la capacitación de los profesores en formulación, implementación y evaluación de proyectos.
Se realizó 1 evento de ESPOLCIENCIA..
Se publicaron 2 títulos de la Revista Tecnológica.
La ESPOL asignó al fondo del CICYT por lo menos $150.000 para la ejecución de proyectos semillas.
Se publicó al final del 2003 una estadística de todos los proyectos de investigación que se realizan en la Institución.

2004: Se aprobó la propuesta conjunta con las Unidades Académicas para la formación de Ph.D., tiempo de investigación e investigaciones en Año Sabático y pasantías.
Se realizaron 2 eventos para la capacitación de los profesores en Gestión de la Investigación.
Se realizó 1 evento de ESPOLCIENCIA..
Se publicaron dos títulos de la Revista Tecnológica.
La ESPOL asignó al fondo del CICYT $200.000 para la ejecución de proyectos semillas.
Se publicó al final del 2004 una estadística de todos los proyectos de investigación que se realizan en la Institución.

Fuente de Financiamiento

VLIR, Proyecto Ancón, FUNDACYT, Empresa Privada, Banco Mundial.

Objetivo 16
Publicar los avances y resultados de los proyectos de investigación en los órganos de difusión internos y en revistas indexadas

Desafío / Tarea

Las Unidades Académicas y Centros de la ESPOL publicarán los avances y resultados de sus proyectos y tesis con una adecuada metodología científica y una presentación y formato de rigor intelectual.

Lineamientos Básicos

- ✓ Todas las Unidades Académicas de la ESPOL tendrán Coordinadores de Investigación y promoverán la publicación de sus tesis y resultados de investigación.
- ✓ Las Tesis de Graduación y los Proyectos de Investigación y Desarrollo tendrán publicaciones como artículos de rigor científico-académico.
- ✓ El CICYT promoverá la publicación de revistas especializadas por áreas académicas.
- ✓ El Consejo de Investigación controlará la calidad y rigor de las publicaciones internas.
- ✓ Habrá reconocimiento diferenciado para los profesores y estudiantes que publiquen en Revistas Internas e Indexadas.

Indicadores de Éxito

2004: Edición y publicación de la Revista Investigación y Desarrollo, 1 por año.
Edición y publicación de la Revista Tecnológica, 2 veces por año.

Fuente de Financiamiento

Proyecto Ancón.

Objetivo 17
Publicar libros de ayuda a la Educación Superior y otros ligados a la investigación y desarrollo en la ESPOL

Desafío / Tarea

Las Unidades Académicas de la ESPOL, en coordinación con el CICYT, se unirán en equipos multidisciplinarios para publicar libros especializados en temáticas de la realidad nacional.

Lineamientos Básicos

- ✓ Las Unidades Académicas, en concordancia con el CISE y el CICYT, publicarán textos educativos de gran aporte a la sociedad.
- ✓ El CICYT promoverá y coordinará la formación de equipos técnicos y científicos que publicarán libros de aporte fundamental y de aplicación a la industria y sector empresarial del Ecuador.

Indicadores de Éxito

2004: Se publicó al menos 2 libros, siendo uno de ellos educativo y el otro técnico, científico y de desarrollo.

2005: Se publicó al menos 4 libros: Dos de ellos de materias de educación y dos de aporte técnico-científico con incidencia social.

Fuente de Financiamiento

Proyecto Ancón.

Objetivo 18
Impulsar y desarrollar la creatividad para Proyectos de Innovación Tecnológica

Desafío / Tarea

La ESPOL participará activamente en el programa de FUNDACYT y otros para Proyectos de Innovación Tecnológica.

Lineamientos Básicos

- ✓ El CICYT, en conjunto con las unidades académicas, presentará proyectos de Innovación Tecnológica de FUNDACYT.
- ✓ La ESPOL contribuirá con Innovación Tecnológica a proyectos de demanda social urgente como vivienda, salud, educación, alimentación, energía, comunicación y otros.
- ✓ ESPOL-Ciencia promoverá un Concurso de Creatividad.
- ✓ La ESPOL participará en la Feria Nacional de Ciencias, promoviendo y difundiendo las promociones que realizan.
- ✓ El CICYT trabajará en el fortalecimiento del Museo y Centro Interactivos de Ciencias.

Indicadores de Éxito

2003: En la ESPOL habrá al menos 10 concursantes de inventos, para superar el registro anterior.

2004: La ESPOL presentó 10 proyectos de Innovación Tecnológica en el FUNDACYT.
La ESPOL participó en el Concurso de Innovación Tecnológica Internacional y en la Feria de Ciencias a realizarse en Quito.
Se realizó una Feria del Museo y Centro Interactivo de Ciencias, con al menos, 50 exhibits totalmente implementados.

Fuente de Financiamiento

ESPOL, VLIR.

Objetivo 19

Promover y financiar investigaciones que generen invenciones susceptibles de ser explotadas, y crear las condiciones institucionales para generar ingresos provenientes de patentes, marcas registradas y otras formas previstas en las leyes ecuatorianas

Desafíos/Tareas

CICYT formulará el borrador del Instructivo que aprobará el Rectorado.

Lineamientos Básicos

- ✔ En la sociedad del conocimiento es un imperativo garantizar la "propiedad intelectual" como elemento para atraer inversión y obtener ingresos.

- ✔ La Ley de Educación Superior incluye como parte del patrimonio de las universidades y escuelas politécnicas *'los ingresos provenientes de patentes y marcas registradas como fruto de sus investigaciones "y los beneficios obtenidos por su participación en empresas productoras de bienes y servicios"*.

- ✔ La misma Ley manda que *"los docentes que hayan intervenido en una investigación tendrán derecho a participar, individual o colectivamente, de los beneficios que obtenga el centro de educación superior de la explotación o cesión de derechos sobre las invenciones realizadas"*.

- ✔ Es deber de las universidades y escuelas politécnicas "desarrollar las actividades de investigación científica en armonía con la legislación nacional de dencia y tecnología y la Ley de Propiedad Intelectual".

- ✔ La ESPOL ha dado especial énfasis en transferir y comercializar tecnologías, como parte de sus vínculos con la comunidad y poner el conocimiento al servicio del desarrollo.

Indicadores de Éxito

2004: Aprobado y difundido el Instructivo.
Número de Patentes.
Número de convenios celebrados con el sector productivo.

CAPITULO III
GESTION DE LAS TICs

20. Ofertar a todos los estudiantes, profesores y trabajadores de la ESPOL, medios de acceso apropiados a las facilidades que ofrecen las TICs.
21. Propiciar las oportunidades que ofrecen las TICs, de manera que sus servicios cumplan los estándares internacionales.
22. Descentralizar la responsabilidad de la planificación, adquisición, operación y mantenimiento de los recursos tecnológicas especializados, en concordancia con los estándares, políticas del uso de la TICS y los servicios de calidad que oferta la ESPOL.
23. Lograr que todos los estudiantes de la ESPOL adquieran un nivel de competencia en el uso de las TICs, apropiado para sus estudios y vocación.
24. Lograr que la planta de empleados de la ESPOL mantenga un nivel de competencia en el uso de las TICs, apropiado con las actividades que desarrollan en su área.
25. Lograr que la planta docente de la ESPOL mantenga un nivel de competencia en el uso apropiado de las TICs en el aula, y en la actividad académica y de investigación que desarrolla en su área.

Objetivo 20
Ofertar a todos los estudiantes, profesores, y trabajadores de la ESPOL medios de acceso apropiados a las facilidades que ofrecen las TICs

Desafío/Tareas

El CTI y el Centro de Servicios Informáticos (CSI) presentarán al Consejo Politécnico el Plan Estratégico de las TICs.

Lineamientos

- ✔ Es de alta prioridad institucional, dentro de los próximos 5 años, proveer y facilitar a todos los estudiantes, profesores, investigadores y trabajadores de la ESPOL, acceso a las redes de computadoras apropiadas, con sus actividades de enseñanza, aprendizaje, investigación y gestión.
- ✔ El acceso a las TICs será equitativo y no discriminatorio.
- ✔ Se establecerán políticas de financiamiento apropiadas para garantizar la adquisición de tecnología, mejoramiento del ancho de banda, computadoras, equipos de redes y comunicaciones, servicios de acceso y facilidades de impresión.
- ✔ Se propiciará la formación de un consorcio con otras universidades para buscar con la industria de tecnología y las organizaciones financieras, acceso para los estudiantes, al momento del ingreso/registro a la ESPOL.
- ✔ Las unidades académicas dictarán cursos que requerirán el uso de las TICs, proporcionen acceso con costo apropiado a los estudiantes enrolados en esos cursos.
- ✔ La ESPOL continuará negociando y administrando el licenciamiento de software de uso común para profesores, estudiantes y personal.
- ✔ Se arbitrarán medidas para que las facilidades de computación y de conectividad cumplan con los estándares de calidad y los cambios y necesidades de las TICs.

Indicadores

Primer semestre académico 2004: a todos los estudiantes (al momento de registro) y a todos los profesores, investigadores y trabajadores, se les proveerá de una cuenta de acceso permanente con clave (cambiable), de manera que todos los sistemas de bases de datos y fuentes de información de la ESPOL, en Facultades, Institutos y demás Unidades puedan ser accedidos a través de una misma clave.

Segundo semestre del 2004: Todas las aulas y auditorios de la ESPOL tendrán instalados un punto de acceso al backbone de la ESPOL e Internet, de manera que

todos los profesores estén en capacidad de utilizar materiales basados en las TICs para la enseñanza.

Segundo semestre del 2004: un 50% de las aulas y auditorios tendrán capacidad de acceso a tecnología y materiales basados en las TICs, para uso de los estudiantes durante las sesiones de clase.

Segundo semestre del 2004: la ESPOL explorará las necesidades de proveer y mantener las herramientas tecnológicas para los cursos comunes de ingeniería.

Segundo semestre del 2004: El Campus "Gustavo Galindo Velasco" ofrecerá el acceso de manera inalámbrica a todos los estudiantes, profesores, investigadores y trabajadores.

Fuente de Financiamiento

Proyecto Ancón

Objetivo 21

Propiciar las oportunidades que ofrecen las TICs, de manera que sus servicios cumplan los estándares internacionales

Desafío/ Tarea

El CTI y el CSI presentarán al Consejo Politécnico el Plan Estratégico de las TICs.

Lineamientos

- ✔ La ESPOL incorporará en sus planes operativos la provisión de tecnología, servicios de calidad y estándares, y propiciará un ambiente académico en el cual se faciliten nuevas formas de enseñanza e investigación, facilitando eficientemente las comunicaciones entre estudiantes – profesores, y enriqueciendo toda la experiencia de aprendizaje de los estudiantes mientras se encuentran en la ESPOL.

  Este objetivo es central para la internacionalización de la ESPOL, tanto en términos de la calidad de los graduados, como en la percepción externa.

Indicadores

Segundo semestre académico del año 2003: se convirtió el actual sitio WEB en un portal de servicios, que permite difundir de manera efectiva toda la información de la ESPOL.

Fines del año 2003: se elaboró un plan para integrar todas las bases de datos que se manejan en los campus de la ESPOL, para crear una Base de Datos Institucional.

Segundo semestre académico del 2003: el sitio WEB de CSI ofrecerá servicios, tales como, creación interactiva de cuentas de correo electrónico en el servidor GOLIAT, soporte básico para el usuario (instalación de software, revisión de versiones, revisión de impresoras, etc.), servicio de descarga de archivos de software de uso frecuente que los usuarios obtienen de Internet (servicio de download).

Fuente de Financiamiento

Proyecto Ancón

Objetivo 22
Descentralizar la responsabilidad de la planificación, adquisición, operación y mantenimiento de los recursos tecnológicos especializados, en concordancia con los estándares, políticas del uso de la TICS y los servicios de calidad que oferta la ESPOL

Desafío/Tarea

El CTI y el CSI presentarán al Rector el conjunto de recomendaciones para alcanzar este objetivo.

Lineamientos

- ✔ La ESPOL asegurará y proveerá una infraestructura básica de capacidad apropiada.
- ✔ Se asegurará que haya compatibilidad entre tecnología y procedimientos.
- ✔ Se financiarán las iniciativas de innovación en el uso de las TICs.
- ✔ Se crearán incentivos para las iniciativas de uso compartido entre unidades de los recursos tecnológicos e infraestructura.

Indicadores

- ✔ **Fines del primer semestre del 2004**: la ESPOL determinará, con la recomendación del CSI y el CTI, y de acuerdo a las políticas de uso de las TICs, los servicios de tecnología y otras facilidades, que son de responsabilidad primaria de las unidades.
- ✔ **Fines del primer semestre del 2004**: la ESPOL especificará, con la recomendación del CSI y el CTI, los protocolos de comunicación comunes, prácticas y estándares de hardware y software, que aseguren el uso eficaz y simple de las TICs en todos los niveles de la Institución.
- ✔ **Fines del segundo semestre del 2004**: la ESPOL proporcionará financiamiento a las iniciativas patrocinadas por los profesores tendientes a innovar el uso de las TICs en el aula, así como las de uso compartido de los recursos de tecnología e infraestructura entre Facultades y Unidades.
- ✔ **Fines del Segundo Semestre del 2004**: La ESPOL mantendrá, a través de CSI, la administración e instalación de redes, servidores centrales y correo electrónico, para las comunicaciones entre Facultades, Unidades, los otros Campus y con el exterior, pero manteniendo y asegurando accesos comunes.

Fuente de Financiamiento

Proyecto Ancón.

Objetivo 23

Lograr que todos los estudiantes de la ESPOL adquieran un nivel de competencia en el uso de las TICs, apropiado para sus estudios y vocación

Desafío/Tarea

Es responsabilidad de las unidades académicas el desarrollo en los estudiantes de las habilidades relacionadas al uso y aplicación de las TICs.

Lineamientos

- ✔ Todo estudiante de la ESPOL desde el curso prepolitécnico, será entrenado para desarrollar habilidades en el uso de las TICs.
- ✔ Entrenamiento de todos los estudiantes que ya ingresaron, en las habilidades básicas del uso de las TICs.
- ✔ Entrenamiento a los estudiantes en habilidades tecnológicas que las sociedades profesionales y el mercado laboral así lo demanden.

Indicadores

Primer semestre del 2004: la Oficina de Admisión a la ESPOL, entrenará y calificará las habilidades del uso de las TICs a los estudiantes que aspiran ingresar.

Primer semestre académico 2004-2005: las Unidades Académicas continuarán ofreciendo el entrenamiento a los estudiantes en el uso básico de las TICs.

Fuente de Financiamiento

Proyecto Ancón.

Objetivo 24

Lograr que la planta de empleados de la ESPOL mantenga un nivel de competencia apropiado con el uso de las TICs en las actividades que desarrollan en su área

Desafío/Tarea

El CTI presentará el plan de reentrenamiento.

Lineamiento

- ✔ Todo nuevo empleado tendrá, como parte de la inducción, un Programa de Entrenamiento.
- ✔ Todos los empleados profesionales de la ESPOL, recibirán un Programa de Calificación y Entrenamiento en el uso de las TICs, apropiados con las actividades que desarrollan en su área como medio para mejorar la gestión administrativa y la prestación de los servicios institucionales.
- ✔ Se incluirá en los perfiles laborales de la ESPOL, la especificación de las habilidades requeridas en el uso de las TICs, para realizar una tarea.
- ✔ Se propiciará las oportunidades para que todo el personal logre un nivel apropiado de competencia en el uso de las TICs.

Indicadores

Primer semestre del 2004: se desarrolló un programa de inducción general para el nuevo personal que ingresa.

Segundo semestre del 2004: las habilidades en el uso de las TICs se especificaron en las descripciones de tareas que ejecutará el personal.

Fuente de financiamiento

Proyecto Ancón.

Objetivo 25

Lograr que la planta docente de la ESPOL mantenga un nivel de competencia apropiado con el uso de las TICs en el aula y en la actividad académica y/o de investigación que desarrolle en su área

Desafío/Tarea

El CTI presentará el Plan de Reentrenamiento.

Lineamientos

- ✔ Todo profesor que se incorpore a la planta docente de la ESPOL, como parte de la inducción, recibirá un programa de entrenamiento en el uso pedagógico de las TICs.
- ✔ Los docentes de la ESPOL tendrán un Programa de Entrenamiento en el uso pedagógico de las TICs en el aula, apropiados con las actividades que desarrolla en su área.
- ✔ Se incluirá en los perfiles laborales de la ESPOL, la especificación de las habilidades requeridas en los nuevos profesores, en el uso de las TICs, para realizar sus actividades académicas.
- ✔ Se propiciará las oportunidades para que todo el personal docente logre un nivel apropiado de competencia en el uso de las TICs en el aula.

Indicadores de Éxito

Fines del primer semestre del 2004: las habilidades en el uso de las TICs se especificaron en las descripciones de las actividades académicas que ejecutará el profesor.

Fines del primer semestre del 2004: se desarrolló un programa de inducción para los nuevos profesores que ingresan a la ESPOL, y que incluya el entrenamiento en el uso pedagógico de las TICs.

CAPITULO IV
VÍNCULOS CON LA COMUNIDAD

> En el contexto global del desarrollo (económico, sustentable, humano y científico-tecnológico), los programas y proyectos que ejecuta la ESPOL se rigen por los principios siguientes:
> 1) Ganar-Ganar; 2) Complementariedad; 3) Cooperación Interinstitucional; 4) Inclusión; 5) Participación; 6) Equidad Social; 7) Rendición de Cuentas
>
> ESPOL

Objetivos

26. Crear los Centros de Transferencia y Desarrollo de Tecnologías que tengan el apoyo real de los sectores productivos.
27. Implantar el Parque Tecnológico de Guayaquil en el campus "Gustavo Galindo Velasco".
28. Crear las políticas y estructuras para desarrollar el emprendimiento e incubadoras de empresas de base tecnológica en la ESPOL.
29. Liderar la prestación de servicios científico-técnicos y la capacitación de recursos humanos que requieren los sectores productivos y los organismos públicos del Ecuador.
30. Consolidar el Programa de Apoyo a la Península de Santa Elena.
31. Fortalecer la presencia editorial de la ESPOL.
32. Ejecutar proyectos de colaboración recíproca con sectores productivos.
33. Medir, de manera objetiva, sistemática y permanente, la calidad de la prestación de servicios y de los diferentes componentes de la vinculación con la comunidad, e introducir esa tarea como rutinaria en la vida de la ESPOL.

Objetivo 26
Crear los Centros de Transferencia y Desarrollo de Tecnologías que tengan el apoyo real de los sectores productivos

Tareas/Desafío

- ✔ Buscar los Promotores para crear los CTDTs.

Lineamientos Básicos

- ✔ Para cada área fundamental de la economía de la Costa habrá un CTDT.
- ✔ Los CTDTs de la ESPOL se regirán por la Ley de Centros de Transferencia y Desarrollo de Tecnologías, el Reglamento General de los CTDT y las resoluciones del Consejo Politécnico.
- ✔ Los CTDTs funcionarán adscritos al Rectorado y bajo los principios de autofinanciamiento y complementariedad.

Indicadores de Éxito

2004: El Consejo Politécnico aprobó por lo menos 2 CTDTs.

Fuente de Financiamiento

Presupuesto ESPOL, hasta 20.000 dólares por Centro; autofinanciamiento.

Objetivo 27
Implantar el Parque Tecnológico de Guayaquil en el campus "Gustavo Galindo Velasco"

Tarea/Desafío

- ✔ Lograr que, mediante Ley, se cree el Parque Tecnológico de Guayaquil.
- ✔ Atraer, por lo menos, a una multinacional para que se instale en el Parque.

Lineamientos

- ✔ La ESPOL, a través del Rector, liderará el proyecto; buscará el respaldo de todos los sectores políticos, económicos, académicos y cívicos de Guayaquil; y, deberá ganar la adhesión del Presidente de la República y de todos los sectores del Congreso.
- ✔ La ESPOL, promulgada la Ley, hará las inversiones esenciales para atraer a las multinacionales y crear las condiciones materiales de la implantación y desarrollo inicial del Parque (Fase 1).
- ✔ Todo lo relacionado con el Parque estará a cargo de la Fundación prevista en el Proyecto de Ley.

Indicadores de Éxito

2004: EL Congreso aprobó la Ley de Creación del Parque Tecnológico de Guayaquil.

2005: Se inició la construcción de la infraestructura básica de la Fase 1 del Parque; y, se firmó el Convenio con una multinacional.

Fuente de Financiamiento

Presupuesto ESPOL; autofinanciamiento.

Objetivo 28
Crear las políticas y estructuras para desarrollar el emprendimiento e incubadoras de empresas de base tecnológica en la ESPOL

Desafío/Tarea

- ✔ Crear y desarrollar el Centro de Espíritu Emprendedor en el marco del Proyecto VLIR-ESPOL.
- ✔ Crear una Incubadora de Empresas de Base Tecnológica.

Lineamientos Básicos

- ✔ El emprendimiento es un eje transversal en la formación de "profesionales politécnicos" y las unidades académicas tendrán el apoyo institucional pertinente.
- ✔ El Centro de Emprendimiento mantendrá, de manera permanente, relaciones con centros similares de prestigio internacional, y se posicionará como líder en el Ecuador.
- ✔ El emprendimiento es un área fundamental y así se lo considerará para otorgar becas en el extranjero.
- ✔ La ESPOL seguirá colaborando con la Fundación INCOVAL, cuyo propósito es crear una Incubadora de Empresas en Guayaquil.

Indicadores de Éxito

2003: El Consejo Politécnico aprobó la creación del Centro de Espíritu Emprendedor.
El Centro de Espíritu Emprendedor formuló su Plan Estratégico e inició el proceso de posicionamiento nacional.

2004: Se creó en la ESPOL la Incubadora de Empresas de Base Tecnológica.

Objetivo 29
Liderar la prestación de servicios científico-técnico y la capacitación de recursos humanos que requieren los sectores productivos y los organismos públicos del Ecuador

Desafío/Tarea

- ✔ Establecer, en la ESPOL, los lineamientos, reglamentos y más aspectos que norman la prestación de servicios y la capacitación de recursos humanos.
- ✔ Obtener la calificación de la ESPOL como Centro de Capacitación ante el CNCF.
- ✔ Crear CTDTs para cada área fundamental de la economía regional.
- ✔ Definir la instancia responsable de la vinculación.

Lineamientos Básicos

- ✔ La prestación de servicios es una tarea esencial de las unidades académicas y de los centros institucionales con énfasis en la vinculación externa.
- ✔ La capacitación de recursos humanos que se financie con recursos del CNCF será coordinada por el Centro de Educación Continua, para lo cual deberá incorporarse al Sistema Nacional de Capacitación y Formación Profesional; diversificar sus servicios; utilizar las TICs como medio para ofertar y proveer servicios; establecer alianzas con centros internacionales; crear una fluida relación con las unidades y centros de la ESPOL.
- ✔ Motivar a las unidades académicas para que ofrezcan programas de capacitación en el sitio de las empresas y en la modalidad de estudios a distancia.
- ✔ La prestación de servicios y la capacitación de recursos humanos debe fortalecer las relaciones de la ESPOL con los sectores productivos y la comunidad; potenciar las actividades académicas, vinculando la docencia con el quehacer de las organizaciones reales y desarrollando las habilidades, destrezas y valores que los estudiantes requerirán en su futura vida profesional; y, generar recursos económicos para la ESPOL y los profesores, estudiantes y trabajadores que la ejecutan.

Indicadores de Éxito

2003: El Consejo Politécnico aprobó el Reglamento de Prestación de Servicios.
2004: El CNCF calificó a la ESPOL (CEC) como Centro de Capacitación.
El Consejo Politécnico aprobó Plan de Promoción.

Fuente de Financiamiento

Autofinanciamiento

Objetivo 30
Consolidar el Programa de Apoyo a la Península de Santa Elena

Tarea/Desafío

El Rectorado presentará la propuesta de reestructuración de los componentes, en función de las prioridades, aliados y logros.

Lineamientos

- ✔ Se fortalecerá el componente "Calidad de la Educación" incrementando, vía alianzas estratégicas, el número de escuelas y comunidades, y se explorará la posibilidad de incluir cinco colegios (Santa Elena 2; Salinas 1; La Libertad 1; Playas 1), para garantizar la continuidad del proceso.
- ✔ Parte del campus Santa Elena funcionará en Ancón.
- ✔ Se apoyarán actividades fundamentales como el Turismo.
- ✔ Con las peticiones de los actores claves, en especial las Municipalidades, se reestructurarán los componentes.
- ✔ Se buscará presentar, utilizando canje de deuda externa y la cooperación internacional europea, el programa Desarrollo de las Capacidades Locales, el caso de la Península de Santa Elena.

Indicadores de Éxito

2003: La red se integra de 42 escuelas.
2004: Se reestructuraron los componentes; se aprobó la inclusión de los colegios a la red.

Fuente de Financiamiento

Proyecto Ancón; Canje de Deuda; Cooperación Internacional.

Objetivo 31
Fortalecer la presencia editorial de la ESPOL

Tarea/Desafío

Obtener recursos adicionales de auspiciantes para cofinanciar las series.

Lineamientos

- ✔ Establecer alianzas con empresas amigas para que cofinancien la Serie "Dialogando con los Líderes Ecuatorianos del Siglo XXI".
- ✔ Financiar con recursos institucionales la Serie "Nuestros Valores"; "Matemáticas" y las publicaciones del CICYT, así como la revista ESPOL-Propuestas.
- ✔ Establecer alianzas con instituciones de la comunidad para potenciar la producción intelectual de la ciudad.
- ✔ Reconocer el aporte de los intelectuales que publican en las series de la ESPOL.

Indicadores de Éxito

2003: Se publicaron 4 títulos y se creó la Serie "Vínculos con la Comunidad".

2004: Se publicaron por lo menos 8 títulos.

Fuente de Financiamiento

Proyecto Ancón, hasta un máximo de 30.000 dólares anuales; auspicios.

Objetivo 32
Ejecutar proyectos de colaboración recíproca con sectores productivos

Tarea/Desafío

Las unidades académicas y centros presentarán proyectos de interés mutuo con el sector productivo privado o público.

Lineamientos Básicos

- ✔ Los proyectos contribuirán a mejorar la competitividad de las empresas y el país.
- ✔ Serán prioritarios los proyectos vinculados al nuevo modelo de desarrollo regional con base en el conocimiento y los que potencien la vía tradicional de la economía ecuatoriana.
- ✔ Los proyectos serán autofinanciados, parte de convenios relacionados con donación de Impuesto a la Renta o cualquier mecanismo que garantice, además, la sostenibilidad.
- ✔ Los proyectos deben enriquecer la cátedra y la vinculación de los estudiantes a los procesos productivos y a los procesos comunitarios.

Indicadores de Éxito

2004: Se consolidó el proyecto del CIBE con los bananeros.

Fuente de Financiamiento

Autofinanciamiento y donación del Impuesto a la Renta.

Objetivo 33

Medir, de manera objetiva, sistemática y permanente, la calidad de la prestación de servicios y de los diferentes componentes de la vinculación con la comunidad, e introducir esa tarea como rutinaria en la vida de la ESPOL

Desafío/ Tarea

El Instituto de Ciencias Matemáticas diseñará y desarrollará instrumentos para medir la calidad de la Prestación de Servicios y de los diferentes componentes de la vinculación con la comunidad.

Lineamientos Básicos

- ✔ El prestigio institucional está determinado, en parte, por la calidad de los servicios que prestamos. La percepción de los usuarios es casi siempre la realidad.
- ✔ Compendiar las variables que conviene medir.
- ✔ Diseñar los indicadores de calidad y la manera de medirlos.
- ✔ Formular el plan de medición.
- ✔ Obtener resultados y procesarlos para una primera publicación.

Indicadores de Éxito

2004 **Primer semestre:** En nueve meses, a partir de la aprobación del Plan, el ICM publicó los primeros resultados de la gestión de medición de la calidad (pregrado, postgrado e investigación).

Fuente de Financiamiento

Presupuesto ESPOL.

CAPITULO V
BIENESTAR POLITECNICO

OBJETIVOS

34. Garantizar remuneraciones competitivas para profesores y trabajadores.
35. Consolidar el Fondo de Jubilación.
36. Disminuir la tasa de deserción estudiantil causada por la falta de financiamiento para estudios.
37. Reducir los índices de estudiantes que entran en período de prueba.
38. Ampliar la cobertura de las exoneraciones y becas para premiar a los estudiantes de buen rendimiento académico y bajos recursos económicos, así como a los estudiantes que alcancen éxitos deportivos, académicos y culturales y a los que participen en Programas de Vínculos con la Comunidad.
39. Crear el Seguro Estudiantil de Salud.
40. Mejorar la calidad de los servicios de transporte, salud y comedores.
41. Fomentar y diversificar la práctica del deporte.
42. Fomentar y diversificar la práctica del arte y la cultura.
43. Ejecutar el Programa de Readecuación Física y Tecnológica de las aulas.
44. Favorecer la inserción de los profesionales politécnicos en el mercado laboral.

Objetivo 34
Garantizar remuneraciones competitivas para profesores y trabajadores

Desafío

Los Vicerrectores General y Administrativo-Financiero, ejecutarán las correspondientes auditorías académicas y administrativas para determinar los reales requerimientos de recursos humanos por parte de la ESPOL.

Lineamientos

- ✔ Los incrementos de remuneraciones anuales serán, en lo posible, superiores a la tasa de inflación.
- ✔ Promover la participación de profesores y trabajadores en los proyectos de prestación de servicios, como mecanismo efectivo para mejorar el ingreso.
- ✔ Incentivar económicamente a todos los politécnicos que generen ideas, proyectos y realicen gestiones a favor de la ESPOL.
- ✔ Optimar el uso de los recursos y ser austero en los gastos.
- ✔ Crear un sistema de incentivos que premie los resultados positivos, nuevos conocimientos adquiridos, las publicaciones realizadas, descontando la depreciación de los ya existentes.

Indicadores de Éxito

2004: Se ejecutaron las auditorías.
El incremento salarial superó la tasa de inflación.
Se amplió el número de profesores y trabajadores que ejecutan proyectos de prestación de servicios.

Fuente de Financiamiento

Presupuesto General del Estado; Carreras y Programas Autofinanciados, en lo correspondiente.

Objetivo 35
Consolidar el Fondo de Jubilación Complementaria (FJC)

Desafío/Tarea

Definir las nuevas políticas de manejo e introducir los cambios pertinentes al Reglamento.

Lineamientos Básicos

- ✔ El porcentaje de aportación del personal no jubilado durante el año 2004 será del 12% de sus ingresos.
- ✔ Los dineros del FJC que sean prestados a la ESPOL, deberán ser pagados con sus respectivos intereses, los cuales serán negociados previamente.
- ✔ El Fondo será monitoreado, a través de estudios actuariales, cada vez que exista un incremento salarial de los servidores de la Institución.
- ✔ Para apalancar al FJC, se asignará la cantidad de $500,000.oo anuales durante 4 años, a partir del año 2004, con fondos provenientes del proyecto ANCÓN y en concordancia con los resultados de las corridas de simulación realizadas.
- ✔ El 90% de los jubilados de la ESPOL, serán pagados con fondos provenientes del FJC.
- ✔ El Fondo será manejado de manera autónoma por una Comisión Tripartita: ESPOL, profesores y trabajadores.
- ✔ En su manejo financiero se combinará alta seguridad y rentabilidad adecuada.

Indicadores de Éxito

2003: El Consejo Politécnico definió nuevas políticas.

2004: - El Consejo Politécnico reformó el Reglamento, de acuerdo con los lineamientos básicos de este objetivo.
- Se entregaron los $500.000 correspondientes al año 2004.

Fuente de Financiamiento

Ancón y aportes personales de profesores y trabajadores.

Objetivo 36
Disminuir la tasa de deserción estudiantil por falta de financiamiento para estudios

Desafío/Tarea

- ✔ Crear mecanismos que aborden de manera integral las múltiples causas de la deserción estudiantil.
- ✔ Universalizar la información sobre las bondades del IECE, asesorar a los estudiantes en la presentación de las solicitudes de crédito y hacer los seguimientos correspondientes.

Lineamientos Básicos

- ✔ La ESPOL debe crear las condiciones académicas y de bienestar para que, de manera general, todo estudiante que ingresa a la ESPOL alcance un título profesional.
- ✔ Los estudiantes son los primeros clientes de los centros de estudios, sin clientes no hay organizaciones.
- ✔ El diálogo profesor-estudiante es un mecanismo idóneo para reducir la deserción estudiantil.
- ✔ La deserción estudiantil es un indicador complejo de la gestión académica.
- ✔ La deserción está vinculada a la calidad del bachillerato, a la vocación, a situaciones socioeconómicas, a la gestión docente.
- ✔ La deserción estudiantil significa pérdidas económicas para el país y para las familias.

Indicadores de Éxito

2003: Se consiguió $600.000 de créditos del IECE a favor de 250 estudiantes politécnicos.

2004: Se incrementó, por lo menos en un 10%, los créditos del año precedente.
Se disminuyó por lo menos en un 10% la tasa de deserción.

Fuente de Financiamiento

Presupuesto ESPOL (gestión), IECE (crédito).

Objetivo 37
Reducir los índices de estudiantes que entran en período de prueba

Desafío/Tarea

El Vicerrectorado de Asuntos Estudiantiles y Bienestar formulará un conjunto de propuestas operativas para disminuir el número de estudiantes que entran en período de prueba.

Lineamientos Básicos

- ✔ La ESPOL creará las condiciones académicas y de bienestar para que, de manera general, todo estudiante que ingresa a la ESPOL alcance un título profesional.
- ✔ Los estudiantes son los primeros clientes de los centros de estudios, sin clientes no hay organizaciones.
- ✔ Cada estudiante es un ser humano diferente y el análisis debe ser individualizado.
- ✔ El diálogo profesor-estudiante es un mecanismo idóneo para reducir la mortalidad académica.
- ✔ La ESPOL fortalecerá y normará las Consejerías Académicas que servirán para realizar un seguimiento de la trayectoria de los estudiantes en la ESPOL permitiendo reducir el índice de mortalidad académica.

Indicadores de Éxito

2003: Se redujo por lo menos en un 10% el número de estudiantes que entran en período de prueba.

2004: Se incrementó anualmente por lo menos en un 10% los resultados del año precedente.

Fuente de Financiamiento

Presupuesto ESPOL (carga Politécnica).

Objetivo 38

Ampliar la cobertura de las exoneraciones y becas para premiar a los estudiantes de buen rendimiento académico y bajos recursos económicos, así como a los estudiantes que alcancen éxitos deportivos, académicos y culturales y a los que participan en Programas de Vínculos con la Comunidad

Desafío/Tarea

El Vicerrectorado de Asuntos Estudiantiles y Bienestar presentará al Rector, en el primer semestre del 2004, una propuesta para reformar el Reglamento correspondiente, en donde a más de los beneficiarios actuales se incluyan los previstos en los lineamientos.

Lineamientos Básicos

- ✔ El dinero de los estudiantes (incremento de registros) regresa a los estudiantes.
- ✔ En las tecnologías tradicionales, Ciclo Básico e Ingenierías tradicionales se exonerará con el 100% del registro a todos los estudiantes regulares de bajos recursos que aprueben todas las asignaturas (mínimo 4) y cuyo promedio sea superior a SIETE; y, con el 50%, si el promedio está en el rango 6.50-7.00. Se beneficiará a un máximo de 100 estudiantes de las Tecnologías, 150 del Ciclo Básico y 150 de las ingenierías. Total 400.
- ✔ Los estudiantes regulares con P3 y P4 que aprueben todas las asignaturas (mínimo 4) recibirán beca de alimentos en el término siguiente.
- ✔ Se incrementará el porcentaje de exoneración a los estudiantes deportistas y a los ganadores de premios en eventos científicos, técnicos, culturales, artísticos y de naturaleza análoga organizados por la ESPOL o por instituciones de reconocido prestigio.
- ✔ Se duplicará el número de becas de "Equidad y Excelencia" que se financian con fondos del Proyecto Ancón.
- ✔ Se creará la beca de "Gestión Productiva", a favor de los estudiantes que participan en Programas de Vínculos con la Comunidad que sean autofinanciados.
- ✔ Se auscultará la posibilidad de exoneraciones parciales a favor de los hijos de los jubilados politécnicos.

Indicadores de Éxito

2004: El 10% de los estudiantes regulares gozan de exoneraciones y becas.
Se creó la beca de "Gestión Productiva".

Fuente de Financiamiento

Incremento del valor de los registros. Proyecto Ancón.

Objetivo 39
Crear el Seguro Estudiantil de Salud[2]

Desafío/Tarea

El Rectorado, utilizando métodos participativos, negocia la creación del Seguro Estudiantil de Salud.

Lineamientos Básicos

- ✔ El dinero de los estudiantes (incremento de registros) regresa a los estudiantes.
- ✔ Se beneficiará el 100% de los estudiantes regulares.
- ✔ La cobertura será básica.
- ✔ Los costos serán compartidos entre ESPOL y el estudiante.
- ✔ La ESPOL aportará como mínimo 12 dólares/año por estudiante regular.

Indicadores de Éxito

2004: Se firmó el contrato correspondiente y entró en vigencia el Seguro Estudiantil de Salud.

Fuente de Financiamiento

Incremento del valor de los registros; autofinanciamiento (estudiantes).

---

[2] Incluye: Seguro por Muerte Natural, Invalidez Temporal y Permanente, Muerte por Accidente; Asistencia Técnica Médica, Maternidad al 100% (máximo 15 atenciones)

Objetivo 40
Mejorar la calidad de los servicios de transporte, salud y comedores

Desafío/Tarea

El Vicerrectorado de Asuntos Estudiantiles y Bienestar y las empresas pertinentes formulan el Plan de Mejoramiento.

Lineamientos

- ✔ El dinero de los estudiantes regresa a los estudiantes. Se incrementará los registros en igual porcentaje a la inflación y con ese valor se financiarán los costos adicionales de los servicios.
- ✔ Los estudiantes son los primeros clientes de la ESPOL.
- ✔ El servicio de transporte operará con costos reales y la ESPOL subsidiará la reposición de unidades, por cada dólar que aporten los estudiantes la Escuela entregará 2 dólares para reponer por año; 2 vehículos con capacidad para 50 pasajeros. Además, se explorarán varias opciones para obtener recursos, entre ellas publicidad en los vehículos, adhesivos de ingreso, etc.
- ✔ Se mantendrá la cobertura y calidad de los actuales servicios de salud y se incluirá el Seguro Estudiantil de Salud, que es un objetivo específico de este plan.
- ✔ El servicio de bares y comedores se ampliará creando opciones (comidas vegetarianas, rápidas, etc.) sin que implique inversión institucional. Se velará para que se cumplan los estándares de calidad alimenticia.

Indicadores de Éxito

2004: Se compraron 2 vehículos con capacidad para 50 personas.
Se incrementó la oferta de bares y comedores.

Fuente de Financiamiento

Presupuesto ESPOL.

Objetivo 41
Fomentar y diversificar la práctica del Deporte

Tarea/Desafío

Lograr que un organismo externo financie la construcción de un Centro de Alto Rendimiento.

Lineamientos Básicos

- ✔ Se aprovechará al máximo, y de manera planificada, el uso de las actuales instalaciones, sin que afecte la cotidianidad de las actividades académicas.
- ✔ Se reconocerán, mediante exoneraciones, becas y otros mecanismos, los logros de los deportistas en eventos de prestigio nacional e internacional.
- ✔ Se promoverá y fomentará la práctica de los deportes por parte de varones y mujeres, y se pondrá énfasis en fútbol, básquet, volley femenino y en los deportes individuales.
- ✔ Se gestionará para que la ESPOL sea sede de certámenes universitarios y politécnicos.
- ✔ Se apoyará la participación de equipos institucionales en certámenes.
- ✔ Se apoyará la formación de organismos encargados de promover el deporte según estamentos.

Indicadores de Éxito

2003: Se creó el Club ESPOL.

2004: Se inició la construcción del Centro de Alto Rendimiento.
Se ejecutó un certamen femenino interuniversitario en la ESPOL.

Fuente de Financiamiento

Incremento del valor de los registros; Autofinanciamiento, Presupuesto General del Estado hasta 20.000 dólares anuales adicionales.

Objetivo 42
Fomentar y diversificar la práctica del Arte y la Cultura

Tarea/Desafío

Cada año el Vicerrector de Asuntos Estudiantiles y Bienestar presentará, conjuntamente con la dirigencia estudiantil, un Plan de Trabajo, que seguirá los lineamientos siguientes:

Lineamientos

- ✔ Se reconoce que el Arte y la Cultura son elementos indispensables en el proceso formativo de los estudiantes. Se auscultará la posibilidad de que se cree una asignatura opcional sobre Cultura y Sociedad.
- ✔ Como la mayor parte de los estudiantes de la ESPOL están concentrados en el campus "Gustavo Galindo Velasco", la actividad artística y cultural debe adecuarse a esta realidad.
- ✔ Se fomentarán las actividades que fortalezcan la identidad nacional, regional y local en el contexto pluricultural del país.
- ✔ Se apoyarán las iniciativas que presenten los estamentos politécnicos a favor de la práctica y difusión de lo mejor del arte y la cultura nacional y mundial.
- ✔ Se mantendrá la actividad y programas que se ejecutan en el campus Las Peñas.
- ✔ Se trabajará bajo los principios de complementariedad y cooperación interinstitucional con las instituciones públicas y privadas vinculadas al quehacer artístico y cultural.

Indicadores

2004: El Rector aprobó el Plan de Trabajo y asignó los recursos.

Fuente de Financiamiento

Incremento del valor de los registros; autofinanciamiento, Presupuesto General del Estado.

Objetivo 43
Ejecutar el Programa de Readecuación Física y Tecnológica de las aulas

Tarea/Desafío

La Unidad de Planificación, con la colaboración del CTI, presentará el Programa correspondiente con los presupuestos y cronogramas referenciales.

Lineamientos

- ✔ Mejorar el sistema de ventilación de las aulas.
- ✔ Proveer a las aulas del servicio de internet y de facilidades para el uso de las TICs en el aula.
- ✔ Adecuar, en cada unidad académica, aulas para favorecer trabajos grupales.
- ✔ Construir o readecuar áreas para que cada unidad académica tenga por lo menos un aula tipo auditorio de uso múltiple.
- ✔ Los recursos requeridos se obtendrán del Proyecto Ancón y de Fundación ESPOL 50 años.

Indicadores de Éxito

2004: Se aprobó el Programa y se ejecutó en un 25%.

Fuente de Financiamiento

Proyecto Ancón, Fundación ESPOL 50 Años.

Objetivo 44
Favorecer la inserción de los profesionales politécnicos en el mercado laboral

Desafío/Tarea

Crear y desarrollar el Centro de Promoción y Empleo (CEPROEM).

Lineamientos Básicos

- ✔ La misión del Centro es ser el nexo tangible entre los profesionales y unidades académicas de la ESPOL con las empresas e instituciones del sector productivo del país, ya sea en el área privada como en la pública, mediante un sistema de intercambio de oferta y demanda de servicios de recursos humanos, capaces de aportar, con su excelente formación académica, al desarrollo del Ecuador.
- ✔ El CEPROEM es una estrategia complementaria de inserción de los profesionales politécnicos al mercado laboral, que se articula con la estrategia de emprendimiento, cuyo objetivo es convertir a muchos profesionales politécnicos en empresarios.
- ✔ Las principales funciones del CEPROEM son:
  - Promocionar a los profesionales y egresados politécnicos en las diversas empresas e instituciones del sector público y privado del país.
  - Atender los requerimientos de recursos humanos del sector productivo del Ecuador a través de la selección de personal que cumpla con los perfiles exigidos.
  - Mantener bases de datos de profesionales y egresados politécnicos, así como también de las empresas del sector productivo del país.
  - Poner a disposiciones de los profesionales politécnicos, herramientas que permitan actualizar sus respectivas hojas de vida, para la posterior ubicación laboral.
  - Poner a disposición de las empresas del sector productivo del país, herramientas que permitan realizar requerimientos de personal, para ser atendidos de forma inmediata por el CEPROEM.
  - Organizar Encuentros Laborales, en los que se realicen entrevistas de forma masiva a estudiantes de último nivel, egresados y profesionales politécnicos, por parte de empresas que participen en dichos eventos.
  - Organizar Talleres y Seminarios sobre Temas de Dependencia Laboral, para que nuestros egresados y profesionales adquieran conocimientos sobre sus derechos y obligaciones en este campo.
  - Retroalimentar a las diferentes unidades académicas de la ESPOL las necesidades del sector productivo del país, a fin de que sirva de referencia para toma de decisiones frente a futuras reformas curriculares de las carreras.
  - Realizar el estudio de ubicación de graduados.

Indicadores de Éxito

2003: El Consejo Politécnico aprobó la creación del Centro de Promoción y Empleo.
El personal del CEPROEM organizó al menos 1 Encuentro Laboral, para generar demanda de recursos humanos politécnicos.

2004: El CEPROEM consiguió autofinanciamiento de al menos el 50% de su presupuesto anual.
El CEPROEM organizó dos Encuentros Laborales (1 por semestre) y tres Seminarios sobre temas de Dependencia Laboral para los estudiantes de último nivel, egresados y profesionales politécnicos.

Fuente de Financiamiento

2003: Presupuesto ESPOL.
2004: 50 % Presupuesto ESPOL y 50 % Autofinanciado.

CAPITULO VI
GESTION ADMINISTRATIVO-FINANCIERA

> "Lo que no se puede medir, no se puede evaluar, lo que no se puede evaluar, no se puede controlar y lo que no se puede controlar, no se puede mejorar.
>
> **Máxima estadounidense**

45. Redefinir la estructura institucional.
46. Diseñar, implementar y mantener un sistema de gestión de la calidad que cumpla con los requisitos de la norma ISO 9001:2000 y mejorar continuamente su eficacia.
47. Mejorar la calidad del servicio administrativo-financiero para contribuir al desarrollo académico y optimar la atención a los usuarios de la ESPOL.
48. Constituir un fondo de operación que garantice liquidez.
49. Manejar y usar la información como elemento clave de la gestión.
50. Formular y Ejecutar el Programa de Identidad e Imagen Corporativas.
51. Medir, de manera objetiva, sistemática y permanente, la calidad de la gestión administrativa, financiera y los servicios de bienestar politécnico y estudiantil, e introducir esa tarea como rutinaria en la vida institucional.

Objetivo 45
Redefinir la Estructura Institucional

Tarea/Desafío

El Rectorado presentará a la comunidad politécnica los lineamientos del nuevo Estatuto que incluirán una propuesta para redefinir la estructura institucional, en especial organismos de gobierno y unidades académicas.

Lineamientos Básicos

- ✔ Hay que adecuar el Estatuto a las disposiciones de la Ley de Educación Superior.
- ✔ Se deben incluir todas las disposiciones que la Ley reserva para los estatutos.
- ✔ El máximo organismo colegiado debe ser uno diferente a la Asamblea Politécnica, pues hay varias disposiciones legales que tornan a ésta inviable o, por lo menos, disfuncional.
- ✔ El Estatuto solo debe consagrar los aspectos generales de la Institución, en especial lo que hace relación al marco conceptual de los campos de la vida académica; en consecuencia, hay que eliminar lo reglamentarista y lo sujeto a cambios recurrentes.
- ✔ La elección de Rector y Vicerrector General se haría como lo establece la primera parte del Art. 34 de la Ley (así lo dispone el CONESUP).
- ✔ El máximo organismo colegiado debería tener dos responsabilidades básicas:
  a) La dirección institucional: política, académica, administrativa, económica, financiera de la ESPOL; y,
  b) La capacidad de pedir rendición de cuentas a las máximas autoridades de la ESPOL y de sus unidades académicas.

Indicadores de Éxito

2003: Se discutieron los lineamientos.
2004: Se aprobó el nuevo Estatuto y se ejecutó el Plan de Racionalización de Reglamentos, Instructivos y Manuales.

Fuente de Financiamiento

Presupuesto ESPOL, sin costo adicional pues corresponde a la carga politécnica.

Objetivo 46

Diseñar, implementar y mantener un Sistema de Gestión de la Calidad que cumpla con los requisitos de la norma ISO 9001:2000 y mejorar continuamente su eficacia

Desafío / Tarea

La ESPOL gestionará y participará activamente en el proceso de implantación, certificación y mantenimiento del Sistema de Gestión de la Calidad.

Lineamientos Básicos

- ✓ La ESPOL establece la implantación del Sistema de Gestión de la Calidad como una herramienta de competitividad.
- ✓ La ESPOL conformará un comité de alta dirección para supervisar la implantación, mantenimiento y mejora del sistema.
- ✓ La ESPOL se comprometerá a establecer la política y los objetivos de calidad así como de comunicarlos a la comunidad politécnica.
- ✓ La ESPOL contribuirá con los recursos necesarios para implementar y mantener el sistema, así como para mejorar continuamente su eficacia.
- ✓ La ESPOL asumirá el liderazgo del recurso humano, buscando un ambiente interno que propicie la mejora continua del sistema.

Indicadores de Éxito

2003: La ESPOL realizó la contratación de la empresa asesora para el proyecto de implantación del Sistema de Gestión de Calidad en las siguientes áreas:

- ✓ Docencia: Facultad de Ingeniería en Electricidad y Computación.
- ✓ Prestación de servicios: Centro de Estudios de Medio Ambiente.
- ✓ Gobierno Central: Administrativo, Financiero y Recursos Humanos.

2004: La ESPOL alcanzó la certificación de los sistemas de gestión para las tres áreas establecidas y extendió la implantación del sistema a dos unidades académicas y a dos centros de prestación de servicios.

2005: La ESPOL alcanzó la certificación del sistema de calidad para las cuatro nuevas áreas y mantiene la certificación de las primeras áreas mejorando continuamente el sistema.

Fuente de Financiamiento

ESPOL.

Objetivo 47

Mejorar la calidad del servicio administrativo-financiero para contribuir al desarrollo académico y optimar la atención a los usuarios de la ESPOL

Tarea/Desafío

El Vicerrectorado Administrativo-Financiero presentará al inicio de cada año el Plan correspondiente.

Lineamientos Básicos

- ✔ Las actividades administrativas son el soporte de la actividad académica.
- ✔ Los empleados y trabajadores deben brindar a los clientes/usuarios de la ESPOL un servicio de calidad y calidez.
- ✔ La capacitación, adquisición de nuevas destrezas y los cursos de pregrado y postgrado son oportunidades para todos los trabajadores que cumplen sus responsabilidades laborales y los requisitos académicos de admisión.
- ✔ Los procesos administrativos y financieros estarán definidos expresamente a través de los manuales y cumplirán obligatoriamente las normas legales, y los reglamentos internos y pasos no harán engorrosos los procedimientos.
- ✔ El número de servidores deberá adecuarse a los requerimientos del desarrollo académico y al uso cotidiano de las TICs en los procesos administrativos-financieros.
- ✔ Se mejorarán los ambientes de trabajo, lo que incluye acciones para favorecer la autoestima personal, imagen de las oficinas, modernización de equipos, calidad y elegancia de los uniformes.
- ✔ Se creará un sistema de incentivos (becas, reconocimientos, etc.) que premien a los trabajadores o unidades que contribuyan al cumplimiento de este objetivo.
- ✔ Se fomentará la implementación de los estándares de medición de desempeño pertinentes.
- ✔ Se reinsertará en el sistema educativo a los trabajadores que no han alcanzado el bachillerato.

Indicadores de Éxito

2004 Se diversificó la capacitación considerando las propuestas de los trabajadores. Se introducirá cambios en los procesos a cargo de la Dirección Financiera, lo cual quedará establecido expresamente en los manuales de procesos que corresponde.

Fuente de Financiamiento

Presupuesto ESPOL .

Objetivo 48
Constituir un Fondo de Operación que garantice liquidez

Desafío/Tarea

La Dirección Financiera presentará al Rectorado el estudio correspondiente.

Lineamientos

- ✔ Se nutrirá del incremento de la producción del Proyecto Ancón y de la Prestación de Servicios.
- ✔ Debe garantizar por lo menos 45 días de funcionamiento institucional.
- ✔ Debe garantizar el pago cumplido de las remuneraciones.

Indicadores de Éxito

2004: Consejo Politécnico aprobó la creación del Fondo y asignó los recursos.

Fuente de Financiamiento

Proyecto Ancón.

Objetivo 49
Manejar y usar la información como elemento clave de la gestión

Desafío/Tarea

Mejorar la calidad de la información que maneja la ESPOL para permitir tomar decisiones en el campo académico, administrativo, financiero, de extensión, etc. de manera más eficaz y oportuna.

Lineamientos Básicos

- ✓ El elemento común en todas las actividades cotidianas que realizamos profesores, servidores administrativos y estudiantes es la información.
- ✓ La generación y manejo de la información absorbe considerables recursos económicos. Estos gastos pueden disminuir si mejoramos el uso de las TICs en los diversos procesos de manejo de la Información.
- ✓ Establecimiento de políticas en el manejo de la información con el propósito de disminuir el uso de "papel y fotocopias" e incrementar el uso del computador e Internet.
- ✓ Identificación y estructuración de formas especificas de uso de información.
- ✓ Establecimiento de un Sistema Administrativo Documental.
- ✓ Concentración y control de ciertos documentos e información en una Base de Datos Institucional.

Indicadores de Éxito

2004: Se presentó el Plan por parte del Director del CSI.
Se recopiló y procesó la información por sectores o áreas previamente definidas.
Se establecieron las Bases de Datos y de un Sistema de Control Documental.
Se capacitó al personal.
Se implantó el Sistema de Administración Documental y de Información en la Secretaria General, Biblioteca y diferentes unidades académicas y de apoyo.

Fuentes de Financiamiento

Presupuesto ESPOL.

Objetivo 50
Formular y Ejecutar el Programa de Identidad e Imagen Corporativas

Desafío/Tarea

El Rector formulará el Programa en el año 2004.

Lineamientos

- ✔ Debe contribuir a consolidar la principal fortaleza institucional: su prestigio, la marca ESPOL.
- ✔ En la formulación se utilizarán métodos participativos que recojan la percepción y expectativas de todos los estamentos politécnicos, de los aliados estratégicos y de la sociedad.
- ✔ Lo fundamental es lograr un cambio de actitud y compromisos serios con los estamentos y en especial con los que toman decisiones para alcanzar los objetivos del Programa.
- ✔ Se utilizarán las TICs para difundir el Programa.

Indicadores de Éxito

2004: Consejo Politécnico aprobó el Programa y se lo difunde de manera masiva utilizando las TICs.
Todas las publicaciones de la ESPOL utilizan los logotipos, colores y símbolos que la caracterizan.

Fuente de Financiamiento

Presupuesto ESPOL.

Objetivo 51

Medir, de manera objetiva, sistemática y permanente, la calidad de la gestión administrativa, financiera y los servicios de bienestar politécnico y estudiantil, e introducir esa tarea como rutinaria en la vida institucional

Desafío/ Tarea

Diseñar y desarrollar instrumentos para medir la calidad de gestión.

Lineamientos Básicos

- ✔ Servir a los clientes con calidad, calidez y a tiempo, es un deber de toda institución.
- ✔ Diseñar los indicadores de calidad y la manera de medirlos.
- ✔ Formular el plan de medición.
- ✔ Obtener resultados y procesarlos para una primera publicación.

Indicadores de Éxito

2004: Primer Semestre: En nueve meses a partir de la aprobación de Plan, el ICM publicará los primeros resultados de la gestión de medición de la calidad de esta gestión.

Fuente de Financiamiento

Presupuesto ESPOL.

CAPITULO VII
INFRAESTRUCTURA FISICA

Una de nuestras fortalezas es poseer una infraestructura física funcional, diversa y con un campus excepcional: el "Gustavo Galindo Velasco"

OBJETIVOS

52. Asegurar el desarrollo armónico del campus "Gustavo Galindo Velasco" y preservar su integridad.

53. Transformar el campus Las Peñas en un complejo académico, cultural, urbanístico y de servicios.

54. Realizar las adecuaciones físicas en el campus Santa Elena.

55. Ejecutar las adecuaciones físicas que requiere el campus Daule.

Objetivo 52

Asegurar el desarrollo armónico del campus "Gustavo Galindo Velasco" y preservar su integridad

Desafío/Tarea

- ✔ Obtener los recursos económicos necesarios para hacer las construcciones y la reforestación.
- ✔ Lograr que mediante ley se cree el Parque Tecnológico.

Lineamientos

- ✔ Se construirán con recursos propios, autogestión y cooperación internacional los siguientes edificios: Ciclo Básico, Electrónica, Mecánica, CTI, Asociación de Profesores, Asociación de Trabajadores, Asociación de Estudiantes, Biblioteca y Residencia Estudiantil.
- ✔ Se mejorarán las vías internas del campus, para lo cual se buscará apoyo interinstitucional y el mecanismo de donación del impuesto a la renta.
- ✔ La reforestación en lo posible se hará con recursos externos y autofinanciados; se centrará en el área del Cerro Azul y deberá incluir los componentes de albarradas y turismo ecológico.
- ✔ Se firmarán contratos de comodatos que contribuyan al desarrollo armónico del campus; que preserven su integridad físico-ecológica; y, que brinden opciones para contar con un Auditorio o Aula Magna, un Centro Cultural.
- ✔ Se auscultará la posibilidad de crear un Parque Industrial que contribuya al desarrollo de las manufacturas y a la creación de pequeñas, medianas y grandes empresas industriales.

Indicadores de Éxito

2003: Se completaron los estudios de los edificios y vías, y se reconstruyó la vía interna.

2004: Se construyó el edificio de Ciclo Básico.
La Unidad de Planificación presentó los estudios de prefactibilidad de creación del Parque Industrial.

Fuente de Financiamiento

Recursos institucionales, Fundación ESPOL 50 Años.

Objetivo 53
Transformar el campus Las Peñas en un complejo académico, cultural, urbanístico y de servicios

Desafío/Tarea

Tener el estudio de factibilidad.

Lineamientos

- ✔ El campus Las Peñas guardará correspondencia con "Malecón 2000", el desarrollo urbano del sector y los requerimientos de la ESPOL (se sugirió que funcionen en él los Postgrados, Educación Continua y Centros que establezcan una relación más estrecha con los sectores productivos).
- ✔ El Proyecto debe autofinanciarse, para lo cual incluirá un área de propiedad horizontal.
- ✔ El proyecto debe garantizar a la ESPOL el dominio a perpetuidad del campus, excepto al área de propiedad horizontal.
- ✔ El Rector liderará las negociaciones para financiar el proyecto.

Indicadores de Éxito

2004: Concluyó el estudio de factibilidad.

2005: Se inició la transformación del campus Las Peñas.

Fuente de Financiamiento

Autofinanciado.

Objetivo 54
Realizar las adecuaciones físicas en el campus Santa Elena

Desafío/Tarea

Los directivos correspondientes, con el apoyo de la Unidad de Planificación presentarán al Rectorado el Plan de Adecuaciones con las respectivas propuestas, fuentes de financiamiento y cronograma.

Lineamientos básicos

- ✔ En las actuales instalaciones funcionarán las carreras de Computación, los programas de Inglés y los que aprobare el Consejo Politécnico.
- ✔ En Ancón funcionará la carrera de Pesquería.
- ✔ La fuente de financiamiento será el Programa de Apoyo al Desarrollo de la Península de Santa Elena.

Indicadores de Éxito

2003: Se aprobó e inició el Plan.
2004: Se ejecutó todo lo previsto para el 2004.

Fuente de Financiamiento

Proyecto Ancón, Programa de Apoyo al Desarrollo de la Península de Santa Elena.

Objetivo 55
Realizar las adecuaciones físicas que requiere el campus Daule

Desafío/Tarea

El Centro Politécnico Daule, con el apoyo de la Unidad de Planificación, presentará al Rectorado el Plan de Adecuaciones con las respectivas propuestas, fuentes de financiamiento y cronograma.

Lineamientos Básicos

- ✔ Se priorizará, en el tiempo, la readecuación de aulas, laboratorios y servicios.
- ✔ Se incluirán obras que vinculen educación con producción, como parte del proyecto de emprendimiento que promueve la ESPOL.
- ✔ Se considerará la posibilidad de crear el Centro de Tecnologías Apropiadas para el arroz, en el contexto de las alianzas estratégicas con los sectores productivos y el Estado (silos de ENAC).
- ✔ Se articularán varias acciones a las expectativas de los actores claves del cantón expresados en el Plan Estratégico de Daule, como lo relacionado con el camal, el centro agro turístico, la agricultura orgánica.
- ✔ Las fuentes de financiamiento del plan deben ser múltiples, pues los recursos fiscales asignados a ESPOL son limitados.

Indicadores de Exito

2004: Se aprobó e inicio del Plan de Readecuaciones.

Fuente de Financiamiento

Presupuesto ESPOL, autofinanciamiento.

Anexo 4

Entrevistas con autoridades de la ESPOL

Guayaquil, 14 Diciembre 2005

Chang - Noboa - Murrieta
Papel de Trabajo:1

DOMINIOS DE ISO 17799	
Objetivo: Determinar los dominios de mayor importancia para la alta Gerencia Nota: En el la siguiente clasificacion asigne un orden de 1 a 10 de acuerdo a la importanticia de los dominios	
DOMINIOS	ORDEN
Políticas de Seguridad	1
Organización de la Seguridad	2
Clasificación y control de los activos	4
Seguridad del personal	
Seguridad física y medioambiental	
Gestión de comunicaciones y operaciones	
Control de accesos	3
Desarrollo y mantenimiento	
Administración de la continuidad	
Cumplimiento	

Escuela Superior Politécnica del Litoral

ING. ARMANDO ALTAMIRANO CHAVEZ
Vicerrector General

Ing. Armando Altamirano
Vicerrector General - ESPOL

OBJETIVOS DE CONTROL PARA EL DOMINIO POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	
OBJETIVO	ORDEN
Política de Seguridad de la Información	
Documentación de la política de seguridad de la información	
Revisión y evaluación	

OBJETIVOS DE CONTROL PARA EL DOMINIO ORGANIZACION DE LA SEGURIDAD	
OBJETIVO	ORDEN
Infraestructura de seguridad de la información (1 a 7)	
Foro gerencial sobre seguridad de la información	
Coordinación de la seguridad de la información	1
Asignación de responsabilidades en materia de seguridad de la información	3
Proceso de autorización para instalaciones de procesamiento de información	4
Asesoramiento especializado en materia de seguridad de la información	6
Cooperación entre organizaciones	7
Revisión independiente de la seguridad de la información	5
Seguridad frente al acceso por parte de terceros (1 a 4)	
Identificación de riesgos de acceso de terceras partes	
Tipos de Accesos	
Razones para el acceso	2
Requerimientos de seguridad en contratos con terceros	
Tercerización	
Requerimientos de seguridad en contratos de tercerización	

OBJETIVOS DE CONTROL PARA EL DOMINIO CLASIFICACION Y CONTROL DE ACTIVOS	
OBJETIVO	ORDEN
Responsabilidad por rendicion de cuentas de los activos	
Inventario de activos	
Clasificación de la informacion (1 a 2)	
Pautas de clasificación	
Rotulado y manejo de la información	

Guayaquil, 27 Diciembre 2005

Chang - Noboa - Murrieta
Papel de Trabajo:2

DOMINIOS DE ISO 17799	
Objetivo: Determinar los dominios de mayor importancia para la alta Gerencia **Nota:** En el la siguiente clasificacion asigne un orden de 1 a 11 de acuerdo a la importanticia de los dominios	
DOMINIOS	ORDEN
Políticas de Seguridad	3
Organización de la Seguridad de la información	2
Administración de activos	7
Seguridad del recurso humano	6
Seguridad física y medioambiental	9
Gestión de comunicaciones y operaciones	8
Control de accesos	1
Adquisición, desarrollo y mantenimiento de sistemas de información	10
Administración de la continuidad de negocio	4
Cumplimiento	5
Administración de incidentes de seguridad de la información	11

Ing. Jorge Faytong Durango
Vicerrector Administrativo Financiero

Guayaquil, 27 Diciembre 2005

Chang - Noboa - Murrieta
Papel de Trabajo:2

DOMINIOS DE ISO 17799	
Objetivo: Determinar los dominios de mayor importancia para la alta Gerencia Nota: En el la siguiente clasificacion asigne un orden de 1 a 11 de acuerdo a la importanticia de los dominios	
DOMINIOS	ORDEN
Politicas de Seguridad	2
Organizacion de la Seguridad de la Informacion	3
Administracion de activos	7
Seguridad del recurso humano	6
Seguridad fisica y medioambiental	9
Gestión de comunicaciones y operaciones	8
Control de accesos	1
Adquisición desarrollo y mantenimiento de sistemas de informacion	10
Administracion de la continuidad del negocio	4
Cumplimiento	5
Administracion de incidentes de seguridad de la informacion	11

Ing. Jorge Faytong Durango
Vicerrector Administrativo Financiero

OBJETIVOS DE CONTROL PARA EL DOMINIO CONTROL DE ACCESO	
OBJETIVO	ORDEN
Requerimientos del negocio para control de acceso	1
Administración de accesos de usuarios	2
Responsabilidades del usuario	3
Control de acceso a la red	5
Control de acceso a sistema operativo	6
Control de acceso a aplicaciones	4
Computación móbil y teletrabajo	7

OBJETIVOS DE CONTROL PARA EL DOMINIO POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
OBJETIVO	ORDEN
Politica de Seguridad de la Información	
Documentación de la politica de seguridad de la información	
Revisión de la politica de seguridad de la información	

OBJETIVOS DE CONTROL PARA EL DOMINIO ORGANIZACIÓN DE LA SEGURIDAD	
OBJETIVO	ORDEN
Organización interna	
Comité de administración de la seguridad de la información	2
Coordinación de la seguridad de la información	4
Asignación de responsabilidades de seguridad de la información	5
Proceso de autorización para instalaciones de procesamiento de información	6
Acuerdos de confidencialidad	3
Contacto y autoridades	4
Contactos con grupos especiales de interés	8
Revisión independiente de la seguridad de la información	7
Partes externas (Outsourcing)	
Identificación de los riesgos relacionados a partes externas	1
Direccionamiento de la seguridad cuando se trabaja con partes externas	3
Direccionamiento de seguridad en acuerdos con terceras partes	2

OBJETIVOS DE CONTROL PARA EL DOMINIO ADMINISTRACION DE LA CONTINUIDAD DE LOS NEGOCIOS	
OBJETIVO	ORDEN
Aspectos de la administracion de la continuidad de los negocios	
Incluir la seguridad de la información en el proceso de administración de la continuidad de negocio	1
Continuidad del negocio y evaluación de riesgos	3
Desarrollo e implementación de planes de continuidad incluyendo la seguridad de la información	2
Marco del planeamiento de la continuidad del negocio	4
Pruebas mantenimiento y revaloración de los planes de continuidad	5

Guayaquil, 14 Diciembre 2005

Chang - Noboa - Murrieta
Papel de Trabajo:2

DOMINIOS DE ISO 17799	
Objetivo: Determinar los dominios de mayor importancia para la alta Gerencia Nota: En el la siguiente clasificacion asigne un orden de 1 a 10 de acuerdo a la importanticia de los dominios	
DOMINIOS	ORDEN
Politicas de Seguridad ✓	1
Organizacion de la Seguridad ✓	2
Clasificación y control de los activos	
Seguridad de personal	
Seguridad fisica y medio ambiental	
Gestión de comunicaciones y operaciones	
Control de accesos ✓	3
Desarrollo y mantenimiento ✓	4
Administración de la continuidad	
Cumplimiento	

Ing. Washington Medina
Coordinador del CRECE - ESPOL

OBJETIVOS DE CONTROL PARA EL DOMINIO POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	
OBJETIVO	ORDEN
Politica de Seguridad de la Información	1
Documentación de la política de seguridad de la información	2
Revisión y evaluacion	

OBJETIVOS DE CONTROL PARA EL DOMINIO ORGANIZACION DE LA SEGURIDAD	
OBJETIVO	ORDEN
Infraestructura de seguridad de la información (1 a 7)	
Foro gerencial sobre seguridad de la información	
Coordinación de la seguridad de la información	3
Asignación de responsabilidades en materia de seguridad de la información	1
Proceso de autorización para instalación de procesamiento de información	2
Asesoramiento especializado en materia de seguridad de la información	
Cooperación entre organizaciones	
Revisión independiente de la seguridad de la información	
Seguridad frente al acceso por parte de terceros (1 a 4)	
Identificación de riesgos de acceso de terceras partes	1
Tipos de Accesos	
Razones para el acceso	
Requerimientos de seguridad en contratos con terceros	
Tercerización	
Requerimientos de seguridad en contratos de tercerización	1

OBJETIVOS DE CONTROL PARA EL DOMINIO CONTROL DE ACCESO	
OBJETIVO	ORDEN
Control de acceso	
Administracion de acceso del usuario	
Inscripción del usuario, manejo de privilegios, manejo de la clave del usuario	
Responsabilidades del usuario (1 a 2)	
Uso de claves, equipo de usuario desatendido	
Control de acceso a redes	
Control de accesos a redes	
Control de acceso al sistema de operacion	
Control de acceso a la aplicacion	
Acceso y uso de sistema de monitoreo	
Computación móvil y telecommuting	

OBJETIVOS DE CONTROL PARA EL DOMINIO DESARROLLO Y MANTENIMIENTO DE SISTEMAS	
OBJETIVO	ORDEN
Requerimientos de seguridad de los sistemas (1 a 2)	
Seguridad en los sistemas de aplicación	
Validación de los datos de salida controles de procesamiento interno autenticación de mensajes validación de los datos de salida	1
Controles criptográficos	
Seguridad de los archivos del sistema	
Seguridad de los procesos de desarrollo y soporte	

DOMINIOS DE ISO 17799	
Objetivo: Consolidar requerimientos de alta gerencia versus gerencia operativa de tecnología **Nota:** En el la siguiente clasificacion asigne un orden de 1 a 11 de acuerdo a la importanticia de los dominios	
DOMINIOS	ORDEN
Políticas de Seguridad	1
Organización de la Seguridad de la información	2
Administración de activos	
Seguridad del recurso humano	
Seguridad física y medioambiental	
Gestión de comunicaciones y operaciones	
Control de accesos	3
Adquisición, desarrollo y mantenimiento de sistemas de información	
Administración de la continuidad del negocio	
Cumplimiento	
Administración de incidentes de seguridad de la información	

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

MBA. Ruth Alvarez
Directora CSI-ESPOL

Anexo 5

Descripción de los sistemas financiero
y académico de la ESPOL

Descripción de Sistemas Financiero y Académico ESPOL

SISTEMA FINANCIERO DE LA ESPOL

Como parte del Plan Informático del año 1995, la ESPOL puso en producción el Sistema Financiero de la ESPOL, mediante el desarrollo del mismo en las instalaciones de CESERCOMP. Para este proyecto, se armó un equipo de desarrolladores de sistemas, integrados por:

- 4 analistas-programadores por parte de IBM
- 10 analistas-programadores por parte de la ESPOL, de los cuales la mayoría de ellos eran estudiantes del último nivel de la carrera de Ingeniería en Computación.

El sistema financiero fue puesto en producción en agosto de 1997, terminado en un 60%, después de un año y medio de desarrollo. El 40% restante, se lo concluyó dos años después, debido a la alta rotación del personal que hubo durante este periodo. El sistema se encuentra operativo y se continúa dando mantenimiento al sistema, ya sea para integrar nuevas funcionalidades o para optimizar las existentes.

El sistema financiero consta de los siguientes módulos, todos ellos integrados:

- Elaboración de la Pro forma Presupuestaria
- Ejecución Presupuestaria
- Contabilidad
- Control de Pagos
- Bancos
- Cobranzas
- Facturación
- Compras
- Bodega
- Activos Fijos
- Seguridades

En el año 1998, se continuó con el desarrollo del sistema de nómina, el mismo que tardó aproximadamente un año. Los módulos de este sistema son:

- Nómina mensual del personal con Nombramiento y Contrato en relación de dependencia
- Nómina para el pago del personal docente con contrato por horas
- Nómina para el pago de ayudantías académicas y de actividades varias
- Nómina para el personal administrativo con contrato de servicios profesionales y órdenes de trabajo

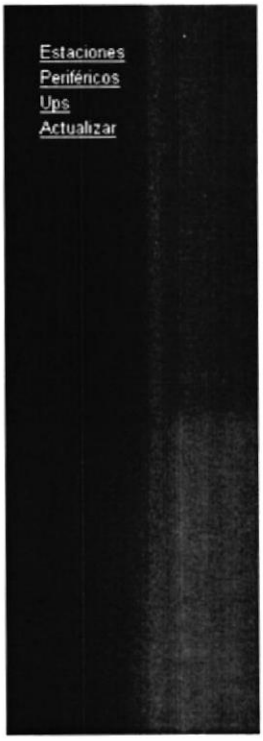
SISTENA ACEDEMICO DE LA ESPOL

El Sistema Académico se puso en producción en el año 1999. El sistema comprende todo lo relacionado al manejo de información académica de pregrado.
Sus funcionalidades son:

- Registros estudiantes
  - Migración de la información del sistema de admisiones con los estudiantes que aprobaron el proceso de admisión
  - Planificación de cursos
  - Control de los flujos académicos por estudiante
  - Control de pre-requisitos, co-requisitos y materias de arrastre
  - Pre-registro y control de pagos de estudiantes
  - Matrícula y Registro de estudiantes
  - Registros estudiantes a través del web (proyecto piloto en octubre de 2004)
  - Convalidaciones y equivalencias
  - Emisión de listas de asistencia
- Control financiero
  - Cálculo del valor del registro para los estudiantes
  - Control de descuentos y exoneraciones
  - Control de valores cancelados en el Banco del Pacífico y la tesorería de la ESPOL
  - Manejo de deudas del estudiantes
  - Control de saldos a favor del estudiante
- Control de ingreso de calificaciones y faltas
  - Manejo de períodos por semestres, bimestres
  - Ingreso de Calificaciones, rectificaciones a través del Web
  - Ingreso de estudiantes que pierden materias por falta a través del web
- Padrones electorales y control de estudiantes que no votaron para aplicar las sanciones establecidas en el reglamento
- Consultas a través del web
  - Historia académica
  - Calificaciones del semestre
  - Deudas
  - Impresión del recibo de pago por concepto de deudas y del registro
  - Actualización de datos personales
- Interfases de información para:
  - Kiosko electrónico
  - Sistema de biblioteca
  - CEPROEM
  - Emisión de carnets
  - Consultas a través del Sistema de Audiorespuesta
  - Software para emitir reportes y obtener información de la base de datos (utilizado exclusivamente por el CRECE)
  - CENACAD, evaluación del personal docente por parte de los estudiantes

Anexo 6

Inventario de hardware de la ESPOL



INVENTARIO DE HARDWARE DE LA ESPOL

Visualización: Por Estaciones

Anterior | Expandir | Buscar | Reportes | Agrupar | Siguiente

Campus Unidad Localización Modelo Cpu Usuario

- Daule
- Gustavo Galindo
- Peñas
  - AEFIMCM
  - BIBLIOTECA
  - CDP
  - CEC
  - CELEX
  - ESPAE
  - FEPOL
  - FIMCM
  - FUNDESPOL
  - LSI
  - Oficina de Ingreso
  - PROTCOM
- Quito
- Santa Elena

Anexo 7

Inventario de software de la ESPOL

LICENCIAMIENTO DE SOFTWARE DE LA ESPOL

Centro de Servicios Informaticos

Soluciones efectivas de Hardware y Software

Principal

Contáctenos

Servicios CSI
Académicos
Administrativos
Inventario de Hardware
Documentos y Formularios

Directorio ESPOL
Solicitud de Creación de Cuentas
Creación de Cuentas
Cambio de Clave
Consulta de Directorio
Actualización de Datos Personales

Guia de Adquisición de Equipos
Computadoras de Escritorio, Portátiles y Servidores
Equipos de Comunicacion

Ayuda
Desconexión del Sistema
Indice de Manuales
Busqueda de Manuales
Consulta AUDIOESPOL
Zona de Downloads
Licencias de Software

Ayuda - Licencias de Software

Convenios para Licenciamiento de la ESPOL

Productos Microsoft

Los productos Microsoft bajo licencia son:

- Todas las versiones del Sistema Operativo Windows
- Office (Word, Excel, Access y Power Point)
- Visio
- Outlook y Outlook Express
- Project
- Visual Studio

Para mayor información consulte la sección Preguntas frecuentes del Convenio Campus Agreement.

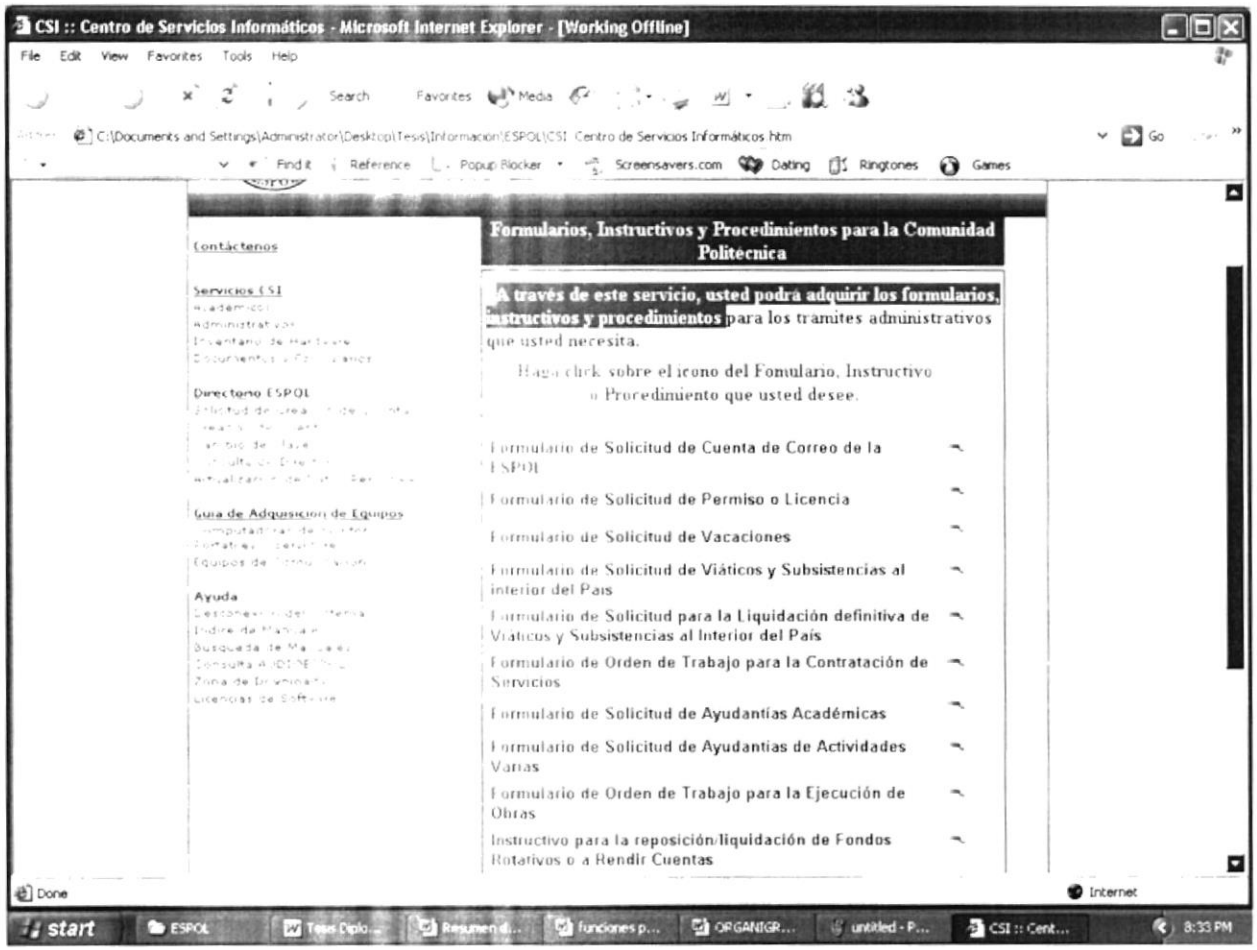
Antivirus Licencia

Smart Letter

Anexo 8

Documentos y formularios

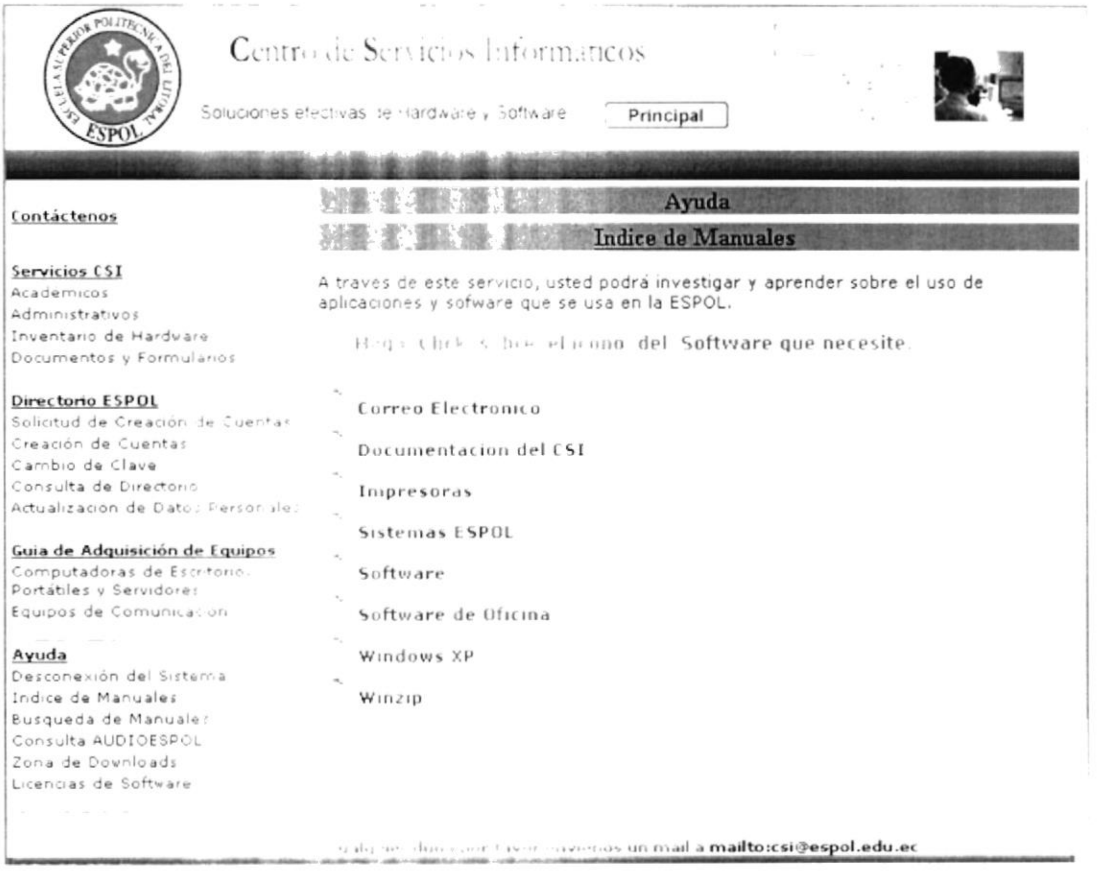
DOCUMENTOS Y FORMULARIOS



Anexo 9

Índice de manuales

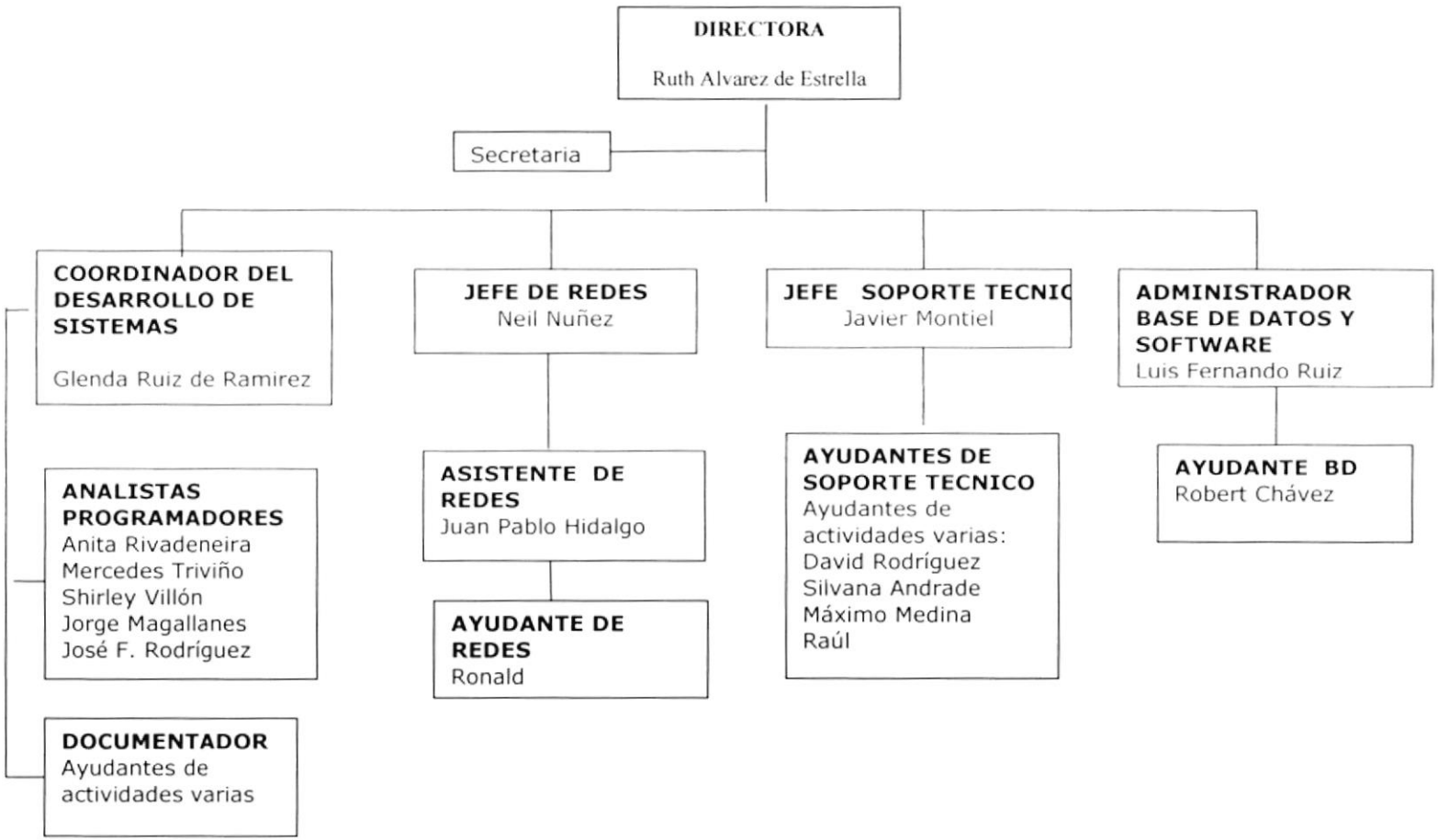
Índice de Manuales



Anexo 10

Organigrama del Centro de Servicios
Informáticos de la ESPOL

ORGANIGRAMA DEL CENTRO DE SERVICIOS INFORMÁTICOS



Anexo 11

Funciones y responsabilidades
del personal del CSI

Funciones y responsabilidades del personal del CSI - ESPOL

DIRECTOR DEL CENTRO DE SERVICIOS INFORMATICOS

Pre-requisitos: Postgrado en Administración, en Ingeniería en Computación o Sistemas, con experiencia en administración de servicios informáticos..

Descripción: Planificar y dirigir todas las actividades del centro de servicios informáticos y organizar los recursos a fin de brindar un servicio eficiente a los usuarios

Reporta a: Rector de la ESPOL

Supervisa a: Coordinador de desarrollo de sistemas, Jefe de Redes, Jefe del Dpto. Técnico.

RESPONSABILIDADES:

- Garantizar la prestación de servicios de tecnología eficientes, de acuerdo a las necesidades de los usuarios internos y externos de la institución
- Informar al Rector sobre los requerimientos y proyectos de expansión del centro en armonía con los planes de la institución.
- Formular proyectos y programas que promuevan el desarrollo tecnológico de la Institución
- Proyectar los requerimientos del CSI incluyendo personal, equipos y demás elementos necesarios, con una estimación de costos de acuerdo a los planes de trabajo.
- Evaluar la aplicación de nuevas tecnologías según los planes y objetivos del CSI y de la Institución
- Definir normas y políticas que regulen los servicios informáticos ofrecidos por el centro.
- Colaborar con las demás áreas en el desarrollo de proyectos tecnológicos de interés institucional.
- Seleccionar y supervisar el personal a su cargo
- Atender el desarrollo y el entrenamiento técnico del personal a su cargo
- Cumplir las demás funciones designadas por la autoridad competente.

COORDINADOR DEL DESARROLLO DE APLICACIONES

Pre-requisitos: Poseer estudios superiores en Ingeniería y/o Análisis de Sistemas, con conocimientos en Administración de proyectos.

Descripción: Planificar, coordinar y dirigir las actividades de desarrollo de sistemas.

Reporta a: Director del CSI

Supervisa a: Analistas y programadores

RESPONSABILIDADES:

- Dirigir las actividades de desarrollo y mantenimiento de sistemas velando que se cumplan con las especificaciones de seguridad e integridad de los sistemas y datos.
- Desarrollar políticas y normas de programación que armonice con los sistemas operativos y ambientes de desarrollo utilizados en el CSI.
- Planificar y administrar la asignación de recursos para el desarrollo, mantenimiento y operación del sistema.
- Establecer un cronograma en la asignación de recursos y las prioridades involucradas en los proyectos de desarrollo de sistemas y en los servicios de soporte.
- Atender necesidades de información y datos, solicitadas por usuarios y/o unidades administrativas y académicas.
- Asignar y supervisar las funciones del personal a su cargo.
- Coordinar las actividades con el DBA para mantener la integridad de los datos.
- Coordinar con los usuarios la implantación de cambios en los sistemas que respondan a las necesidades institucionales.
- Implantar soluciones informáticas eficientes y de calidad, que garanticen su correcto funcionamiento.
- Reportar a la Dirección los avances logrados en los proyectos e implantaciones.
- Cumplir las demás funciones designadas por el Director del CSI

ANALISTA PROGRAMADOR

Pre-requisitos: Conocimiento de análisis y desarrollo de sistemas

Descripción: Análisis, desarrollo y mantenimiento de sistemas de información.

Reporta a: Coordinador del Desarrollo de Aplicaciones

Supervisa a:

RESPONSABILIDADES:

- Analizar las especificaciones de los diseños recibidos.
- Diseñar el flujo lógico de cada programa ajustándolo a las especificaciones y a los estándares recomendados.
- Codificar los programas asignados en el lenguaje indicado.
- Realizar las pruebas y depuración de programas que sean necesarios antes de entregarlos a producción.
- Colaborar directamente en la documentación de los manuales del sistema, de operación y del usuario del proyecto asignado de acuerdo a los estándares establecidos.
- Garantizar el correcto funcionamiento de las aplicaciones desarrolladas.
- Asistir en la capacitación y/o entrenamiento de los usuarios de los sistemas.
- Cumplir las demás funciones designadas por la autoridad competente.

DOCUMENTADOR

Pre-requisitos: Estudios en Análisis de Sistemas ó Ing. en Sistemas. Conocimientos de Procesador de palabras, uso de Hoja Electrónica y Software de documentación.

Descripción: Proveer u obtener la documentación pertinente en las distintas fases de desarrollo de proyectos. Además cumple las funciones de elaboración y custodia de los documentos de la unidad.

Reporta a: Coordinador del Desarrollo de Sistemas

Supervisa a:

RESPONSABILIDADES:

- Participar en el análisis, desarrollo y mantenimiento de sistemas con el fin de recopilar la documentación durante el desarrollo e implantación de las aplicacioes

- Preparar y difundir a las personas pertinentes los documentos preparados.
- Dar soporte con diagramas, gráficos, folletos, esquemas, etc.., a la presentación de trabajos.
- Organizar y custodiar los documentos bajo su responsabilidad.
- Mantener y actualizar los documentos bajo su responsabilidad.

ADMINISTRADOR DE BASE DE DATOS Y APLICACIONES

Pre-requisitos: Ing. en Computación o Sistemas

Descripción: Dirigir las actividades del área de análisis y programación.

Reporta a: Director del CSI

Supervisa a:

RESPONSABILIDADES:

- Diseño, implantar y mantener las Bases de datos de la Institución.
- Desarrollar y administrar las políticas de acceso, estadísticas, encriptación, monitoreo, etc.
- Mantener un alto nivel de seguridad, rendimiento y utilización de las Bases de datos y aplicaciones de la Institución.
- Implantar medidas de control que garanticen la operatividad de las bases de datos y su integridad
- Mantener respaldos de las bases de datos, de tal manera que se garantice la operatividad de la misma en caso de siniestro.
- Mantener un plan de contingencia para recuperación y funcionamiento de la base de datos luego de un siniestro.
- Revisar los resultados de las Auditorías y controles establecidos en la Base de datos y tomar acciones cuando sea necesario.
- Garantizar un adecuado nivel de eficiencia y productividad en las aplicaciones.
- Colaborar con su criterio técnico en las soluciones propuestas por la sección de desarrollo de aplicaciones, y velar por que se cumplan los estándares.
- Documentar los procesos, procedimientos y demás información referente a las bases de datos de la ESPOL.
- Cumplir las demás funciones designadas por el Director de la unidad

JEFE DE SOPORTE TECNICO

Pre-requisitos: Conocimiento en el área de soporte y mantenimiento de equipos de computación

Descripción: Brindar soporte técnico en implantación y mantenimiento de los equipos y programas del Centro de servicios informáticos, así como también supervisar el servicio de soporte a los usuarios de la Institución en el uso de equipos y programas.

Reporta a: Director

Supervisa a: Ayudantes de soporte técnico

RESPONSABILIDADES:

- Planificar y supervisar las actividades de mantenimiento del hardware a su cargo.
- Asesorar a los ayudantes y administradores de las diferentes redes de la ESPOL en el uso, instalación, administración, configuración y mantenimiento de equipos y software.
- Dar soporte a los usuarios en actividades relacionadas al buen funcionamiento del hardware y software
- Asistir al Director en la renovación de contratos de mantenimientos de los equipos y supervisar que se mantengan vigentes.
- Llevar un control del mantenimiento preventivo que los proveedores deben realizar por concepto de contratos de mantenimiento.
- Revisión periódica del generador del CSI (combustible, baterias, agua, aceite, etc), y chequeo de las horas de operación para su respectivo mantenimiento (cambio de filtros, aceite, refrigerantes, etc)
- Mantener actualizado el inventario de Hardware y Software de la Institución.
- Mantener un plan de contingencia para el normal funcionamiento de los equipos, luego de un siniestro.
- Llevar un control del stock y consumo de los materiales de computación y de los productos que se necesitan para el mantenimiento de los diferentes equipos.
- Supervisar las funciones del personal a su cargo.
- Cumplir las demás funciones designadas por la autoridad competente.

AYUDANTE DEL SOPORTE TECNICO

Pre-requisitos: Conocimientos básicos de mantenimiento de computadores y software utilitarios.

Descripción: Brindar soporte técnico en implantación y mantenimiento de los equipos y programas

Reporta a: Jefe de soporte técnico

Supervisa a:

RESPONSABILIDADES:

- Atender los requerimientos asignados por el Jefe del Departamento Técnico.
- Realizar mantenimiento preventivo y correctivo de Hardware y Software a cargo del CSI y de los usuarios que lo solicitaran.
- Actualizar periódicamente el inventario de Hardware y Software de las computadoras de la institución.
- Cumplir las demás funciones designadas por la autoridad competente.

JEFE DE REDES E INTERNET

Pre-requisitos: Ing. Electrónico y/o Computación, con experiencia en el manejo de redes y comuncaciones

Descripción: Brindar soporte técnico en el análisis, diseño y mantenimiento de las redes del Centro de servicios informáticos y de la ESPOL

Reporta a: Director del CSI

Supervisa a: Asistente técnico y ayudantes

RESPONSABILIDADES:

- Diseñar y planificar la infraestructura física y la adquisición de equipos y software para el backbone de la ESPOL y las redes de computadores que se encuentren bajo la administración de CSI, para que el desarrollo de sistemas sea armónico y coherente.
- Administrar la operación y planificar e implementar el crecimiento del backbone y las redes de computadoras, para el suministro de servicios a los usuarios locales y remotos.
- Planificar el desarrollo y la operación de las seguridades del backbone y las redes de la ESPOL
- Desarrollar y documentar procedimientos de administración y control de toda la infraestructura de redes de datos de la Institución.
- Administrar, planificar y desarrollar los servicios de Internet de la ESPOL y toda la infraestructura que esto involucre.
- Asesorar a las unidades de la ESPOL en el diseño de las redes de datos y de la infraestructura requerida para su implantación, con énfasis en la eficiencia y óptimo uso de recursos y seguridades.
- Instruir y coordinar el trabajo de los administradores de las redes de las unidades académicas y administrativas, de tal manera que cumplan con las políticas establecidas por el CSI
- Mantener un plan de contingencia para recuperación y funcionamiento de las redes de datos, luego de un siniestro.
- Supervisar el trabajo del personal a su cargo.
- Cumplir las demás funciones designadas por la autoridad competente.

ASISTENTE DE REDES E INTERNET

Pre-requisitos: Ing. Electrónico y/o estudiante ó egresado del área de Ing. Eléctrica y Computación.

Descripción: Encargará de colaborar en el soporte técnico y administración de los recursos de comunicación y redes e Internet.

Reporta a: Jefe de redes e Internet

Supervisa a:

RESPONSABILIDADES:

- Asistir al Jefe del Departamento de redes e Internet en todas las actividades de administración y mantenimiento de usuarios en las redes de la ESPOL e Internet.
- Administrar los usuarios de Internet.
- Desarrollar y documentar procedimientos de administración y control de toda la infraestructura de redes de datos de la Institución.
- Administrar los recursos destinados para prestar el servicio de Internet.
- Asesorar a los ayudantes y administradores de las diferentes redes de la ESPOL en el uso, instalación, administración, configuración y mantenimiento de las redes.
- Supervisar la instalacion fisica para conexiones de redes
- Garantizar el correcto funcionamiento de los servidores que están bajo la administración de esta unidad
- Cumplir las demás funciones designadas por la autoridad competente.

SECRETARIA DE LA DIRECCION

Pre-requisitos: Bachiller en comercio y administración, especialidad secretariado. Buen conocimiento de la operación de herramientas automatizadas de oficina.

Descripción: Ejecución de labores secretariales y administrativas en la unidad.

Reporta a: Director

Supervisa a: Conserje

RESPONSABILIDADES:

- Elaborar todos los documentos requeridos que se emiten en la unidad y son requeridos por sus superiores
- Controlar la recepción y envío de correspondencia interna y externa; archivar técnica y adecuadamente las comunicaciones generadas y recibidas. Controlar el préstamo de los documentos archivados.
- Atender el teléfono, tomar nota de las instrucciones y novedades, reportar oportunamente la información a los interesados.
- Atender y orientar a toda la comunidad politécnica y al público en general sobre asuntos relacionados con su ámbito de acción.
- Conectar y coordinar las citas, reuniones y eventos relacionados con las labores asignadas a los miembros de su unidad.
- Mantener actualizado y presentar diariamente a sus superiores y al personal de la unidad, el recordatorio de asuntos a cumplirse
- Llevar control administrativo de los requerimientos de materiales.
- Cumplir las demás funciones designadas por la autoridad competente.

Anexo 12

Inventario de riesgos

INVENTARIO DE RIESGOS

CATEGORIA	RIESGO	
Planeación estrategica de sistema	No exista una planeación estratégica de Tecnología de Información acorde a los planes generales de la Empresa	1
	Dificultad de planificar proyectos que involucren tecnología habilitante	2
	No existe un organigrama de la estructura organizacional del personal de Tecnología Información	3
	No exista una política de seguridad de la información formalmente establecida.	4
	Inversión de Hardware y Software no justificable, de acuerdo a los procesos y proyectos de la compañía	5
	No existe control sobre los documentos del centro de cómputo.	6
	Proyectos del área no alineados con los objetivos de la compañía	7
	Retraso tecnológico y por lo tanto desarrollo limitado de la Compañía	8
	No contar con un manual de funciones del personal, o no tenerlo actualizado	9
	Existe una política de seguridad desactualizada.	10
	No contar con un plan de contingencia en el centro de computo	11
	No exista competencia profesional en el personal de IT	12
	No se realice una adecuada selección de nuevo personal	13
	No exista un plan de capacitación del personal de IT	14
	No se encuentre organizada la información de IT	15
	Rotación elevada del personal de IT	16
	Poseer una alto números de proyectos por desarrollarse	17
	Empleado desinformado	18
	Usuario desinformado	19
Políticas de Seguridad de la información	No existe un organigrama de la estructura organizacional del personal de Tecnología Información o que no se encuentre actualizado.	20
	No exista una política de seguridad de la información formalmente establecida.	21
	Exista una política de seguridad de la información que no ha sido conocida por todo el personal.	22
	No contar con políticas y procedimientos respaldos y de recuperación de información.	23
	Exista una política de seguridad de la información no alineada con los objetivos de la organización.	24
	No existe control sobre los documentos del centro de cómputo.	25
	Existe una política de seguridad desactualizada.	26

Políticas operacionales	No existen procedimientos / controles para modificación del software	27
	Existen tapes defectuosos	28
	Existen cartuchos no rotulados	29
	Existe pérdida de cartuchos	30
	No existen procedimientos de respaldo	31
	No existen procedimientos de recuperación	32
	No existe control de los cartuchos	33
	No existe control de envío de cartuchos por valija	34
	No se realiza una revisión de los respaldos (backups)	35
	No existe control sobre los documentos del centro de cómputo	36
	Existen errores de procesamiento	37
	Daño o pérdidas de respaldos de información por almacenamiento indebido	38
	No tener documentación adecuada que respalde las operaciones realizadas	39
	Aplicaciones de procedimientos erróneo al momento de generar los respaldos o de recuperar la información	40
Control de accesos	No existen políticas para la creación de passwords	41
	No existen procedimientos de actualización periódica de passwords	42
	No existen perfiles de usuarios definidos	43
	No poseen sistemas de cifrado de passwords	44
	Divulgación de password, o que los password se encuentre a la vista de todos	45
	El formato de password (número de carcacteres alfanumericos) no sea el adecuado	46
	No se verifica el acceso no autorizado a computadoras del personal	47
	No se tiene instalado software antivirus en las computadoras	48
	No se realiza una actualización periódica del	49
	No se realiza una exploración periódica de virus	50
	No existen procedimeintos para soporte a	51
	Posible incursión de hackers en el sistema	52
	No se encuentre activado el área de log en donde se registre el acceso a los sistemas	53
	No exista el personal encargado de la revisión del área de log de acceso al sistema	54
	Incursión de terceros malintencionados pueden tener acceso a aplicaciones críticas o a datos valiosos por medio del uso de las debilidades en el software de comunicaciones y protocolos	55
	Las aplicaciones o programas solo interactuen con lo necesario de la base de datos más no con el total de la misma.	56
	No exista un mecanismo adecuado que valide el acceso a los sistema desde la parte externa(Confirmación de llamada, verificación de la redundancia)	57
	Solo exista un personal encargado de las claves	58
	No detectar oportunamente accesos indebidos o posibles violaciones de seguridad en la base de datos	59
	Manipulación de los datos de la Base Datos por parte de usuarios no autorizados (modificaciones o eliminaciones)	60
	Imposibilidad de identificar las autorizaciones y motivos de los cambios realizados por Ausencia de pistas de auditorias	61
	Extracción de información confidencial	62

Responsabilidades de usuarios	Divulgación de password, o que los password se encuentre a la vista de todos.	63
	Divulgacion de direccion de correo electronico o de informacion confidencial por internet.	64
	Uso de software ilegal, no autorizado, pirata o	65
	Ingenieria Social.	66
	Spam.	67
Acceso Fisico	Personal no autorisado accese al centro de computo	68
	No exista chapas de seguridad electrica u otro mecanismo de control de ingreso en el area de servidores	69
	No se registren los ingresos del personal al centro de computo en una bitacora	70
	No se cambie periodicamente codigos de acceso digitales si existiera esta tecnologia en el centro de computo	71
	Existe un responsable de la seguridad del acceso fisico al centro computo	72
	Que en la politica de seguridad no se considere el acceso fisico al centro computo	73
	Exista solo una persona encargada de las llaves del centro de computo	74
	El área de servidores no sea la adecuada en el centro de computo	75
	No existan las respectivas señales de advertencia de acceso o emergencias en el centro de computo	76
	Las puertas y ventanas del centro de computo no queden abiertas al final de un dia de laboral	77
	No se encuentre separada las áreas de desarrollo con la de producción	78
	Exista material facilmente inflamable en el centro de computo	79
Bases de Datos	No exista un responsable de la administración de la Base de Datos	80
	Manipulación de los datos de la Base Datos por parte de usuarios no autorizados (modificaciones o eliminaciones)	81
	Imposibilidad para evaluar la validez de la transacción debido a posibles manipulaciones de la base de datos, por ausencia de pistas de auditorias	82
	No se encuentre separada la bases de datos en producción de la bases de datos pruebas	83
	Que este desintalado el log del sistema operativo	84
	Que el administrador de bases de datos no revise el área de logs	85
	No se respalde periodicamente la base de datos	86
	Los cambios sobre la bases de datos no pasen por una previa aprobación	87
	Las aplicaciones o programas solo interactuen con el total de la base de datos más no con lo necesario	88

Desarrollo de Proyectos	Existan proyectos que no justifiquen su razon del por que desarrollarse	89
	No existe una respectiva planificación y aprobación de los proyectos	90
	No exista una persona que sea la responsable de llevar acabo el proyecto	91
	No exista una buena segregacion de funciones en las etapas del desarrollo de los proyectos	92
	Que el analista de sistema tenga acceso a los datos operativos	93
	Personal de programación tenga acceso al área de bilioteca de programas de sistemas	94
	Las pruebas de los programas no se efectuen independientemetne de las pruebas de los sistemas	95
	No exista una documentación adecauda que respalde el trabajo realizado en cada una de las etapas del proyecto	96
	No se mantenga un registro de las modificaciones realizadas en los programas	97
	Se realicen modificaciones sin aprobaciones	98
	Las modificaciones realizadas afecten a los datos o a otros programas	99
Desastres	Incendio	100
	Inundación	101
	Terremoto	102
	Tormenta intensa	103
	Sunami	104
	Ataque terrorista	105
	Altercados/disturbios civiles	106
	Corrimiento de tierras	107
	Avalancha	108
	Accidente industrial	109
	Corte del suministro eléctrico	110
	Error de hardware	111
	Interrupción de la red	112
	Error de los controles medioambientales	113
	Accidente de construcción	114
	No existen generadores eléctricos	115
	No existen UPS's con las computadoras	116
Hardware & Software	Deficiencia en el control de los equipos computacionales que se encuentran asegurados y posibles pérdidas económicas en caso de que exista un contingente con algún equipo no asegurado	117
	Incumplimiento del contrato de leasing por parte de la Compañia que está obligada a asegurar los equipos arrendado	118
	Pérdida de hardware por no contar con un respectivo Inventario	119
	Paralización de las actividades por caídas de servidores, equipos de comunicaciones y equipos personales	120
	Daños o corrupción de datos por fallas electricas.	121
	Daños de los equipos o errores de procesamiento por sobrecalentamiento de los procesadores por falta de ventilación	122
	No tener una adecuada ubicación de los servidores en el centro de computo	123
	No tener una adecuada ubicación del centro de computo	124

Continuidad del Negocio	No exista un plande contingencia formalmente aprobado y documentado	125
	No exista un responsable del plan de contingencia	126
	Las personas no conozcan que hacer al momento de presentarse una contingencia	127
	No se revise periodicamente el plan de contingencia	128
	No se halla realizado las pruebas respectivas del plan de contiengencias	129
	No exista un sitio computo alterno de trabajo	130
Aspecto Legales	Incumplir requisitos legales	131
	Mantener software sin licencias	132
	No cumplir la "Ley de la transparencia de la información"	133

Anexo 13

Asignación de Probabilidad vs. Impacto
a riesgos aplicables

Control de Accesos	Control de Acceso	No exista chapas de seguridad eléctrica u otro mecanismo de control de ingreso en el área de servidores			✓					✓	
		No se registren los ingresos del personal al centro de computo en una bitácora				✓				✓	
		No se cambie periódicamente códigos de acceso digitales si existiera esta tecnología en el centro de computo				✓				✓	
		No exista un responsable de la seguridad del acceso físico al centro computo			✓					✓	
		Que en la política de seguridad no se considere el acceso físico al centro computo									
		Exista solo una persona encargada de las llaves del centro de computo			✓						
		El área de servidores no sea la adecuada en el centro de computo									
		No existan las respectivas señales de advertencia de acceso o emergencias en el centro de computo			✓					✓	
		Las puertas y ventanas de centro de computo queden abiertas al final de un día de laboral									
		Personal de programación tenga acceso al área de bibliotecas de programas de sistemas		✓							
	Control de acceso a la aplicación	Posible incursión de hackers en el sistema									
		No se encuentre activado el área de log en donde se registre el acceso a los sistemas									
		No exista el personal encargado de la revisión del área de log de acceso al sistema			✓					✓	
		Incursión de terceros malintencionados pueden tener acceso a aplicaciones críticas o a datos valiosos por medio del uso de las debilidades en el software de comunicaciones y protocolos de red. (incluido red inalámbrica)		✓							✓
		No exista un mecanismo adecuado que valide el acceso a los sistema desde la parte externa(Confirmación de llamada, verificación de la redundancia)			✓					✓	
		Las aplicaciones o programas solo interactúen con lo necesario de la base de datos más no con el total de la misma.			✓					✓	

MBA. Ruth Alvarez

Anexo 14

Ejemplo de carta de certificación de un SGSI
Banco de Montreal

CERTIFICATE OF REGISTRATION

Information Security
Management System

This is to certify that

Bank of Montreal
Technology and Solutions
Enterprise Infrastructure
4100 Gordon Baker Road
Toronto
Ontario
Canada
M1W 3E8

Hold Certificate No: IS 92770

and operate an Information Security Management System [illegible] complies with the requirements of ***BS 7799:PART 2:2002*** *for the following scope:*

The provisioning of trusted and managed information security services to internal and external customers of the Bank of Montreal (BMO) Financial Group in accordance with the Statement of Applicability dated 22 February 2005

For and on behalf of BSI Inc:

Gary L. Pearson

President

Originally Registered: 7 Apr 2005 *Latest Issue:* 11 **Apr** 2005 *Expiry Date:* **6 Apr 2008** *Page:* 1 of 1

UKAS
INFORMATION SECURITY MANAGEMENT
003

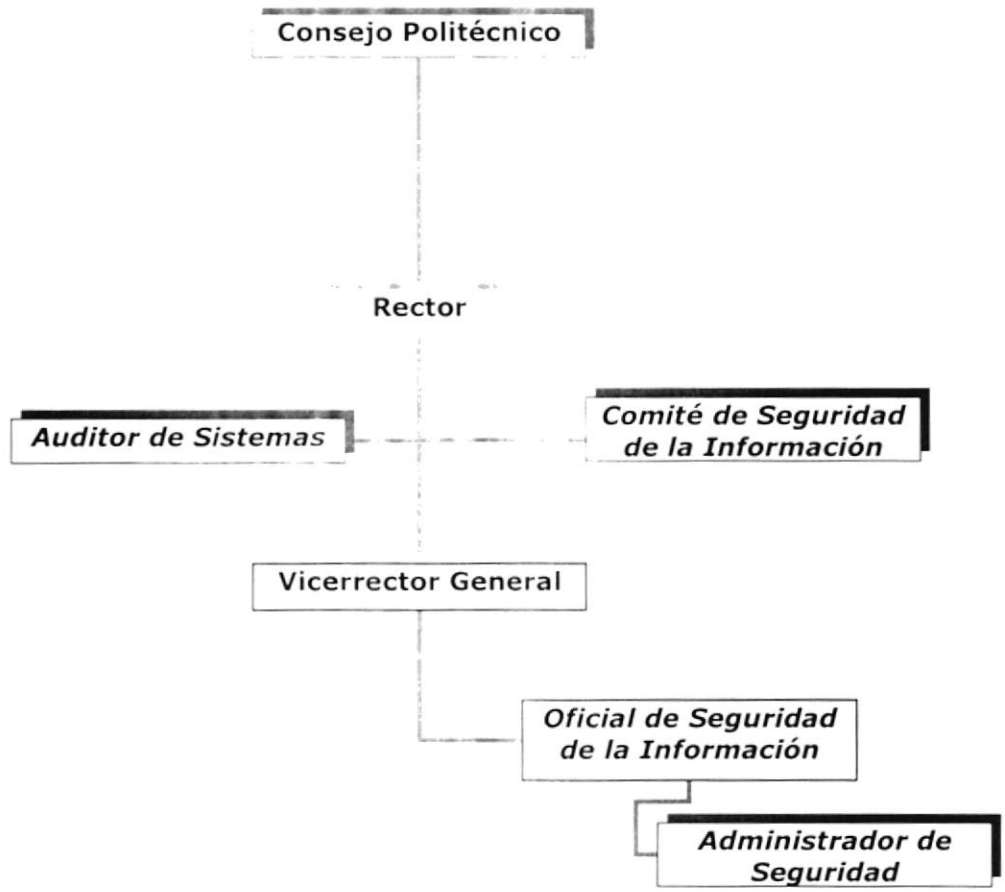
BSi
Management Systems

Anexo 15

Funciones recomendadas para la implementación del Sistema de Gestión de Seguridad de la Información

Roles y funciones recomendadas para la implementación del Sistema de Gestión de Seguridad de la Información en la ESPOL

Roles sugeridos vistos en el organigrama actual de la ESPOL



Las funciones de los roles sugeridos se detallan a continuación.

Comité de seguridad de la información

FUNCIONES:

1. Revisar y proponer a la máxima autoridad del organismo para su aprobación, la Política y las responsabilidades generales en materia de seguridad de la información.
2. Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
3. Tomar conocimiento y supervisar la investigación y el monitoreo de los incidentes relativos a la seguridad.
4. Aprobar las principales iniciativas para incrementar la seguridad de la información.
5. Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
6. Garantizar que la seguridad sea parte del proceso de planificación de la información.
7. Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
8. Promover la difusión y apoyo, a la seguridad de la información dentro de la ESPOL.
9. Coordinar el proceso de administración de la continuidad de las operaciones de los sistemas de tratamiento de información de la ESPOL frente a interrupciones imprevistas.

Oficial de Seguridad de la Información

FUNCIONES:

1. Mantener las reglas de acceso a los datos y a otros recursos de TI.
2. Mantener la seguridad y la confidencialidad sobre la emisión y mantenimiento de las identificaciones de usuario y contraseña.
3. Monitorear las violaciones de seguridad y aplicar acciones correctivas para asegurar que se provea la seguridad adecuada.
4. Revisar y evaluar periódicamente la política de seguridad y sugerir a la gerencia los cambios necesarios.
5. Preparar y monitorear el programa de concientización en seguridad para todos los empleados.
6. Probar la arquitectura de seguridad para evaluar la fortaleza de la seguridad y para detectar las posibles amenazas.

Administrador de Seguridad de Información

FUNCIONES:

1. Realizar tareas operativas relacionadas con la seguridad de la información en concordancia con los lineamientos establecidos por las autoridades de la ESPOL y el Oficial de Seguridad de la Información.

Auditor de Sistemas

FUNCIONES:

1. Participación en el desarrollo de nuevos sistemas:
Evaluación de controles.
Cumplimiento de la metodología.
2. Evaluación de la seguridad en el área informática.
3. Evaluación de suficiencia en los planes de contingencia.
    Respaldos,
    Prever qué va a pasar si se presentan fallas.
4. Opinión de la utilización de los recursos informáticos.
    Resguardo y protección de activos.
5. Control de modificación a las aplicaciones existentes.
    Fraudes
    Control a las modificaciones de los programas.
6. Participación en la negociación de contratos con los proveedores.
7. Revisión de la utilización del sistema operativo y los programas utilitarios.
    Control sobre la utilización de los sistemas operativos
    Programas utilitarios.
8. Auditoria de la base de datos.
9. Auditoria de la red de teleprocesos.
10. Uso de software de auditoria.
11. Apoyo a la auditoria financiera.